### PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2002-132583

(43)Date of publication of application: 10.05.2002

(51)Int.CI.

G06F 12/14 G11B 20/10

(21)Application number: 2000-320548

(22)Date of filing:

20.10.2000

(71)Applicant :

**SONY CORP** 

(72)Inventor:

YOSHINO KENJI ISHIBASHI YOSHITO

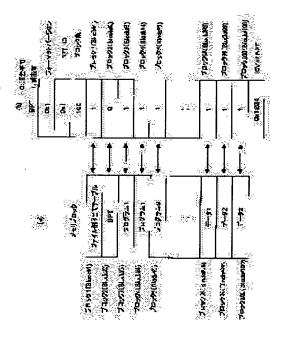
AKISHITA TORU SHIRAI TAIZO ITO TAKESHI

HAYASHI SHIGEKAZU

# (54) DATA PROCESSING APPARATUS, DATA STORAGE DEVICE AND DATA PROCESSING METHOD, AND PROGRAM PROVIDING MEDIUM

#### (57)Abstract:

PROBLEM TO BE SOLVED: To provide a data processing apparatus which is capable of enhancing protection of data stored in data storage means. SOLUTION: For example, in access to the data storage means of a memory card having a flush memory, a block permission table(BPT) being an access permission table is set in a memory interface part of a device. The access to the storage means is performed only when processing is permitted in the BPT, and the processing is not performed for a processing request in violation of the BPT. Since the access to the storage means is always performed according to the table which is set in the memory interface regardless of processing contents in a control part and command, for example, data rewrite in storage media prohibiting the rewrite is prevented effectively.



#### **LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

## **BEST AVAILABLE COPY**

(12) (10) 日本国格紹介 (1 b)

3 擞 ধ 盐 华 噩 4

特開2002-132583

(11)特許出版公開報母

(P2002-132583A)

(43)公開日

平成14年5月10日(2002.5.10)

デーマント・(粉粉)

310A 5B017 5D044

12/14 20/10

G 0 6 F G11B

> G06F 12/14 G11B 20/10

(51) Int.Cl.?

金6頁) **報査開求 末部水 耐水項の数22 OL** 

000002185 (11) 出版人 **存顧2000-320548(P2000-320548)** 平成12年10月20日 (2000.10.20) (21) 出版群中 (22) 出版日

東京都品川区北岛川6丁目7番35号 ソニー株式会社

古野 異治 (72) 発明者

安庆特品川区北岛川6丁目7 435年 一株式会社内

71

石版 做人 72) 発明者

東京都島川区北岛川6丁目7番35号 一株式会社内

バ

(外2名) **炸理儿 山田 英治** 100101801 (74) 代理人

最終買に扱く

データ処理装備、データ記憶装備、およびデータ処理方法、並びにプログラム提供媒体 (54) [発明の名称]

<u> モーブルであるプロック・パーミッション・テーブル</u> ・(BPT)をセットして、BPTにおいて許可された処 手段に対するアクセスが実行されるので、例えば書き換 【解決手段】 例えばフラッシュメモリを搭載したメモ て、デバイスのメモリインタフェース部にアクセス許可 し、BPTに塩反する処理要求に対しては処理を行なわ ない。他は他の処理内容、ロマンドにかかわらず、発行 えを禁止している記録メディア内のデータ音き換えが効 【联題】 データ記憶手段に記憶したデータの保護を高 メモリインタフェースに設定したテーブルに従って記憶 リカード等のデータ記憶手段に対するアクセスにおい 理である場合にのみ配像手段に対するアクセスを実行 めることを可能としたデータ処理装置を提供する。 (57) (開約)

1534 : ı ۰ >0802640*€* DO 1 OI TAB ۱×٥ ι×ο 1:第云可 1:第云可

26-4 : TT4606 176606 140 4.) 写 fd\$ 4. (=)

果的に防止される。

るメモリインタフェースと、数メモリインタフェースの (請求項1] データ記憶手段に対するアクセスを実行す 制御を実行する制御部とを有するデータ処理装置であ (特許請求の範囲)

否を判定し、前配アクセス昨可テーブルにおいて許可設 定のなされた処理のみを集行する構成を有することを特 前記メモリインタフェースは、前記データ記憶手段内の モリインタフェース内にセットし、前記制御部からの前 <u> 記データ配像手段に対するアクセス命令に応じて、前記</u> データ格制領域に格的されたアクセス胜可デーブルをメ アクセス許可テーブルを参照してアクセス命令の東行可 徴とするデータ処理装置。

各々が予め定められたデータ容量を持つ複数セクタから なるブロックを複数有するフラッシュメモリであり、「机 記アクセス許可テーブルは、プロック単位でのデータの ルード数を含れたプロック単位での処理的可能様に従って、プロック単体での処理的可能様に従って、プロック単体での第一 【請求項2】 前記データ記憶手段のデータ格納領域は、 ることを特徴とする静水項しに配転のデータ処理装置。 処理許可堪様を設定したテーブルとして構成され、

合にのみ、前記アクセス命令に応じた処理を実行し、一蔵 「静水項3」 前記メモリインタフェースは、前記制御部 からのアクセス命令に応じた処理が前記アクセス許可デ ーブルにおいて許可数定のなされた処理範囲内である場 アクセス命令に応じたメモリインタフェース内での処理 前記制御部は、前記メモリインタフェースにおける処理 成功フラグの設定の確認を条件として、制御部側の処理 を実行する構成を有することを特徴とする請求項1に記 戦のデータ処理装置。

成功に応じて処理成功フラグを設定し、

【群水項4】 前記制御部は、前記アクセス命令がデータ ファイルの銃み出し処理である場合において、前配デー 夕配位手段内のデータ格納領域に対応して設定されたフ アイル割り当てテーブルから既み田し対象データファイ ルのアドレスを選択し前記メモリインタフェースに送信 する処理を実行し、

し、データ競み出し可能領域である場合にのみデータ競 み出し処理を実行する棉成を有することを特徴とする欝 前記メモリインタフェースは、前配制御部から受信した 税み出し対象データファイルのアドレスに基づいて前配 アクセス許可テーブルを参照して、域アドレスの設定さ れた領域がデータ説み出し可能領域であるか否かを判定 水項1に記載のデータ処理装配。

夕記僚手段内のデータ格納領域の智き込みアドレスを選 【請求項5】 前配制御部は、前配アクセス命令がデータ ファイルの音き込み処理である場合において、前記デー 択し前記メモリインタフェースに送信する処理を実行

ブルを参加して、一畝アドレスの段店された保険がデータ 鲁き込み可能領域であるか否かを判定し、デーク都含込 **10記込モリインタフェースは、前配何創部から受信した** み可能領域である場合にのみデータ費食込み処理を実行 する地成を有することを始散とする請求項」に配放のデ 前記音さ込みアドレスに基づいて前記アクセス許可テー 一夕処理袋匠。

値として、餃テーブル内データに払づいて生成される改 (精水項6)、加配アクセス昨可テーブルは、 威アクセス 件可テーブル内のデータ改成の有無を検査するチェック 欧チェック値 (1 CV)を付帯データとして有し、

工义之を実行する暗号処理節を有し、一般時号処理節にお モリインタフェースに設定し、設定したアクセス推可テ CV)に基づいて、前記アクセス昨可テーブルの改成デ はる前配アクセス胜可テーブルの改成なしの判定が得ら 一ブルに従ったアクセス可否の判定に基づくデータ処理 を実行する構成を有することを特徴とする群状項1に配 前記メモリインタフェースは、前記改成チェック値(1 れたことを条件として、前部アクセス胜可テーブルを必 ゲータ処理装**置。** 

**件可テーブル内のデータ改成の有紙を検査するチェック** 其として、「岐テーブル内データと、「前配データ配位手段 国有の戦別子。(1.ロ)」とを含むデータに基づいて生成さ (請求項7] 前記アクセス許可テーブルは、餃アクセス れる改成チェック値 (1 C V) を付帯データとして有

とを条件として、前記アクセス許可テーブルをメモリイ アルが正当なメディアに格納されているか否かの位証処 **唱として英行され、破検証により正当性の確認されたこ** 1る構成を有することを特徴とする語状型1に記載のデ ンタフェースに数定し、数定したアクセス許可デーブル に従ったアクセス巨的の世所に払びヘアータ処国や状行 (1 C V) に基づく検胚処理は、前配アクセス酢甲デー **竹記メモリインタフェースによる巾配改菓チェック値** プルのデータ改竄チェックに加え、酸アクセス作用デー 一夕処理袋圈。

たことを条件として、前記データ配位手段のメモリに格 粒されたアクセス許可テーブルを前記メモリインタフェ [翳水項8] 前記メモリインタフェースは、前記データ 一ス内にセットする構成を有することを特徴とする観象 日億年段との相互認証処理を実行し、相互認証が成立 項上に配斂のデータ処理装置。

モリであり、前記アクセス許可テーブルは、ブロック単 れたデータ容量を持つ複数セクタを1プロックとしたブ [語水項9] 前記データ記憶手段は、各々が予め応めら ロックを複数有するデータ格納領域を持つフラッシュメ 位でのデータ消去の可否、またはプロック単位でのデー タ再生の可否の少なくともいずれかを設定したテーブル **前記メモリインタフェースは、前記アクセス昨可テープ** 

有することを特徴とする糖求項1に配載のデータ処理装 従って、プロック単位での処理の可否を判定する構成を またはブロック単位でのデータ再生の可否の設定情報に ル中に設定されたプロック単位でのデータ消去の可否、

(請求項10) 各々が予め定められたデータ容量を持つ 複数のセクタを 1 ブロックとした複数ブロックのデータ 格制領域を有するデータ記憶装置であり、

一夕格時間転に格納したことを特徴とするデータ記憶銭 国・ する許可難様を設定したアクセス許可テーブルを前配デ 加配データ格納領域のブロック単位エのデータ処理に関

【精水項11】 前起アクセス許可テーブルは、

前記データ格納領域における前記アクセス許可テーブル を格約したブロックに関するデータ処理許可期様を消去 不可知域として設定した協成であることを特徴とする語 東項10に記載のデータ記憶装置。

**タ処理装置に転送する処理を実行する構成を有すること** 【請求項12】前配データ配磁装置は、跛データ配徹装 個とのデータ転送を実行するデータ処理装置との相互認 証処理を実行する暗号処理部を有し、相互認証が成立し たことを条件として、アクセス許可テーブルを前配デー を特徴とする賭求項10に記載のデータ記録装置。

の制御を実行する制御部とを有するデータ処理装置にお 【路求項13】データ配管手段に対するアクセスを実行 するメモリインタフェースと、蚊メモリインタフェース けるデータ処理方法であり、

前記メモリインタフェースは、

前記データ記憶手段内のデータ格納領域に格納されたアクセス軒可デーブルをメモリインタフェース内にセント するステップ

加設制知能からの加設テータ部権手段に対するアクセス 有名に成じて、加設アクセス群のモースルを終版して、 クセス作金の英位回答条制定するステンプと、前紀アク セス件ロテーブルにおいて作可数定のなされた処理の多

を其行することを特徴とするデータ処理方法。

は、各々が平め定められたデータ容量を持つ複数セクタ り、加配プクセス許可テーブルは、プロック単位でのデ 「請求項14」前記データ記憶手段のデータ格納領域 からなるプロックを複数有するフラッシュメモリであ 一之の処理的可障様を設定したデーブルよして構成さ

(锦坎項15) 加配太王リインタフェースは、前配制御 前記メモリインタフェースは、前記アクセス許可テーブ ル中に設定されたプロック単位での処理許可閣様に従っ て、ブロック単位での処理の可否を判定することを特徴 とする崩水項13に配販のデータ処理方法。

部からのアクセスの会に応じた処理が前記エクセス特可

デーズルにもいて<br />
性可数<br />
定のなされた<br />
処理<br />
処理<br />
の四方<br />
の<br />
方<br />
こ<br />
こ<

数アクセス命令に応じたメモリインタフェース内での処 4台にのみ、前記アクセス命令に応じた処理を実行し、 理成功に応じて処理成功フラグを設定し、 前配制御部は、前配メモリインタフェースにおける処理 **式功フラグの設定の確認を条件として、制御部側の処理** を実行することを特徴とする請求項13に記載のデータ [請求項16] 前記アクセス命令がデータファイルの競 み出し処理である場合において. 的配配的部件 前配データ配像手段内のデータ格納領域に対応して設定 タファイルのアドレスを選択し前配メモリインタフェー されたファイン舞り当てアーブアから親を出し対象デー スに送信する処理を実行し、

前記メモリインタフェースは、

前記制御部から受信した競み出し対象データファイルの て、数アドレスの設定された領域がデータ競み出し可能 領域であるか否かを判定し、データ競み出し可能領域で ある場合にのみデータ銃み出し処理を実行することを特 アドレスに基づいて前記アクゼス許可テーブルを参照し 数とする請求項13に記載のデータ処理方法。

(開水項17),加配了少七公愈完位デー名。2、2、2、4、2、9 き込み処理にある協会において、

机配式一久配位手段内のデータ格的領域の音き込みアド レスを選択し前記メモリインタフェースに送信する処理

て前記アクセス許可テーブルを参照して、貧アドレスの 前記メモリインタフェースは、 前RM(到前から受視した前記書き込みスドレスに基づい 役定された領域がデーク音ぎ込み可能領域であるか否か を判定し、データ智含込み可能領域である場合にのみデ 一夕雪き込み処理を実行することを特徴とする群状項1 3に記載のデータ処理方法。

ク値として、紋テーブル内データに基づいて生成される 【糖求項18】前配アクセス許可テーブルは、餃アクセ ス許可テーブル内のデータ改竄の有無を検査するチェッ 改位チェック値(ICV)を付帯データとして有し、 前記メモリインタフェースは、

前記改竄チェック値(1CV)に基づいて、前記アクセ 前記アクセス許可テーブルの改竄なしの判定が得られた ことを条件として、前記アクセス許可テーブルをメモリ ス許可テーブルの改竄チェックを実行するステップと、 インタフェースに設定するステップと、

設定したアクセス許可テーブルに従ったアクセス可否の を実行することを特徴とする請求項13に配敷のデータ 判定に基づくデータ処理を実行するステップと、

(糖求項19) 前記アクセス許可テーブルは、鈸アクセ ス許可テーブル内のデータ改竄の有無を検査するチェッ

පි

ク値として、餃テーブル内データと、前記データ記憶手 段固有の談別子(1D)とを含むデータに基づいて生成 される改竄チェック値 (1CV) を付帯データとして有

前記アクセス許可テーブルのデータ改竄チェックに加 前配メモリインタフェースは、

**共媒体に関する。** 

破検証により正当性の確認されたことを条件として、前 記アクセス許可テーブルをメモリインタフェースに設定 え、彼アクセス許可テーブルが正当なメディアに格納さ れているか否かの検証処理として前配改度チェック値 (1CV) に基づく検証処理を実行するステップと、 するステップと、

数定したアクセス許可テーブルに従ったアクセス可否の 判定に基づくデータ処理を実行するステップと、

を実行することを特徴とする群求項13に記載のデータ

夕記憶手段との相互認証処理を実行し、相互認証が成立 したことを条件として、前記データ記憶手段のメモリに 格納されたアクセス許可テーブルを前記メモリインタフ ェース内にセットすることを特徴とする請求項13に記 【糖水項20】前記メモリインタフェースは、前記デー 戦のデータ処理方法。

**一夕再生の可否の少なくともいずれかを設定したテーブ** 【精状項21】前配データ配億手段は、各々が予め定め られたデータ 容量を持つ複数セクタを 1 ブロックとした プロックを複数有するデータ格柄領域を持つフラッシュ メモリであり、前配アクセス許可テーブルは、プロック 単位でのデータ消去の可否、またはブロック単位でのデ

従って、プロック単位での処理の可否を判定することを 前記メモリインタフェースは、前記アクセス許可テーブ またはプロック単位でのデータ再生の可否の設定情報に ル中に設定されたプロック単位でのデータ消去の可否、 特徴とする請求項13に記載のデータ処理方法。

の制御を実行する制御部とを有するデータ処理装置にお めるコンピュータ・プログラムを提供するプログラム提 【請求項22】データ配億手段に対するアクセスを実行 するメモリインタフェースと、蚊メモリインタフェース けるデータ処理をコンピュータ・システム上で実行せし 加配データ配依手段均のデータ格的領域に格的されたア クセス許可テーブルをメモリインタフェース内にセッ 供媒体であって、前配コンピュータ・プログラムは、

命令に応じて、前記プクセス軒可デーブルを参照してアー クセス命令の英行可否を判定するステップと、 切記アクセス許可デーブルにおいて許可設定のなされた。 前配削御部からの前配データ配佐手段に対するアクセス

5. 特に、記憶装置に格納されるコンテンツを高度なセ **タ処理装配およびデータ処理方法、並びにプログラム**提 (発明の属する技術分野) 本発明は、データ処理装置お よびデータ処理方法、並びにプログラム提供媒体に関す キュリティ管理のもとに保護することを可能とするデー

い、音楽データ、ゲームプログラム、回像データ邨、様 用器、あるいはゲーム機器においてネットワークから受 格約したメモリカード、CD、DVD等の配位以体を刊 コンテンツ再生処理、あるいはプログラム英行が可能と [従来の技術] 近年のインターネットの忽散な替及、さ 々なソフトデータ(以下、これらをコンテンツ (Conten るいは、DVD、CD、メモリカード毎の配位媒体を介 **宿され記憶媒体に格納されたり、あるいはコンテンツを** () と呼ぶ) の、インターネット毎のネットワーク、あ ユーザの所有するPC (Personal Compuler) 、 再生却 生専用器、あるいはゲーム優器に装整することにより、 **した抗菌が釣増している。これらの院園コンテンツは、** らにモバイル型の小型再生器、ゲーム器等の結及に停 (00003)

あったが、フラッシュメモリは、全ピット一招哨去方式 [0003] コンデンツの記憶繋子として、 仮近多く利. モリは、EEPROM (Electrically Erasable Program により1ピットを1トランジスタで実現することが可能 用される発子にフラッシュメモリがある。フラッシュメ mable ROM)と呼ばれる電気的に雪き換え可能な不揮死性 トを3個のトランジスタで構成するために、1ピット当 たりの占有面積が大きく、集徴度を高くするのに限界が スク等の記録媒体に代わりうるものとして期待されてい メモリの一形態である。従来のEEPROMは、1ピッ となった。フラッシュメモリは、楫処ディスク、光ディ

パクトディスク:登母商爆) 、MD (ミニディスク:発 **母商場) 等のディスク状媒体に換えてメモリカードを**使 【0004】フラッシュメモリをデータ配録/再生機器 **に対して着脱自在に枯成したメモリカードも知られてい** 用するディジタルオーディオ配録/再生装留を契現する る。このメモリカードを使用すれば、従来のCD(コン ことができる。

セットされる。その結果、ファイルサイズを可変長とす [0005] このような、フラッシュメモリを使用した C)、再生器等において使用する場合、FAT(File Al localionTable)システムと呼ばれるファイル管理システ その中に必要なパラメータがファイルの先頃から慰告に ムがアクセス惰頓テーブルとして一般的に使用される。 FATシステムでは、必要なファイルが定義されると、 コンデンツ記憶珠子をパーンナルコンピュータ(P

€

ることができ、1ファイルを1または複数の管理単位

を有式ることを特徴と式るプログラム提供媒体。

(発明の詳細な説明)

処理のみを実行するステップと、

(セクタ、クラスタ等)で協成することができる。この管理単位の関連事項がFATと呼ばれるデーブルに告かれる。このFATシステムは、記録媒体の物理的格性とあ、従って、FATシステムは、記録媒体の物理的格性とあ、従って、FATシステムは、プロッピー(登録高級)ディスク、ハードディスクのみならず、光磁気ディスクにおいても採用することができる。上述したメモリカードにおいても、FATシスケム域用されている。「日本の様々なコンテンは、再生機器として利用される再生機配、ゲーム優報・PC等の情報機器本体からのコーザ間系、あるいは機能されたメカ手段を介したコーザの指示により、上述のFATに基づいて例えば上述したフラッシュメモリから呼び出され、情報機器本体、あるいは機能されたディスプレイ、スピーか等を通じて再

(0008)ユーザに対する利用的限を実現する1つの 事性が、配布コンテンツの略号化処理である。すなわ ち、例えばインターネット等を介して時号化された音句 データ、回線データ、ゲームプログラム等の含価コンデ ンツを配布するとともに、正規ユーザであると傾認され た者に対してのみ、配布された時号化コンテンツを復身 力る手段、すなわち近号総を付与する構成である。 (0009) 路号化データは、所反の手続きれる。 の呼によって利用可能な値号データ(平文)に戻すこと ができる。このような情報の暗号化処理に暗号化総を用い、彼号処理に偏号化とをでき

00100

「現明が解決しようとする課題」例えばパーソナルコン ピュータ(PC)のOSのファイルシステムが生体的に 配録メディアに格納されているアクセス僧順テーブルと してのFAT(File Allocation Table)を読み込んで 管理する協成においては、PC側のファイルシスデムが そのアクセス情報デーブルであるFATの内容を自由に 毎き換えてしまうという処理が可能であった。

(0011)従って、例えば曾込み禁止佞域を認定したアクセス情報テーブル(PAT)により管理されたコンテンツを格的した記録メディアがあっても、そのアクセス情報デーブルをPC側のファイルシステムが観みとって曾き銭えてしまうことが可能であり、本来、曾む技えを禁止している記録メディア内のデーダ(コンデンツ)

の書き換えが可能になってしまい、コンテンツの保護が 十分になされないという久点があった。

を効果的に防止し、コンデンツの保護を高めることを可 ス部に保持させる構成とすることで、制御部の処理内容 る。このように、本発明は、例えば書き換えを禁止して **能としたデータ処理装置、データ配憶装置、およびデー タ処理方法、並びにプログラム提供媒体を提供すること** 【0012】本発明は、上述の従来技術の欠点に鑑みて、 なされたものであり、メモリカード等のデータ配像手段 を装着したデバイスにおいて、予め定められたアクセス 作可情報に基づいた処理についてのみデバイスから記憶 手段に対するアクセスを実行し、アクセス許可信報に遠 た。また、アクセス許可テーブルをメモリインタフェー にかかわらず、常にメモリインタフェースに設定したテ いる記録メディア内のデータ(コンテンツ)の告き換え ーブルに従って記憶手段に対するアクセスが実行され 反する処理要求に対しては処理を行なわない構成とし を目的とする。

(0013)

(原題を解決するための手段) 本発明の第1の側面は、 データ配准手段に対するアクセスを実行するメモリイン タフェースと、蔵メモリインタフェースの側割を実行す る側切能とを有するデータが理集値であり、加配<u>メモリ、 の域に独的されてプレスを開発を表現のデータ構造 国域に独的されてプレスを開発を表現のデータ構造 国域に独的されてプレスを解す。ファースの構造を スニース内にセットし、和配補創的からの制配データ形 選手段に対するアクセス権可デーが必然でリイグ ロデーブルを砂限してアクセス命令に応じて、前記プウセス財 可デーブルを砂限してアクセス命令に応じて、前記プウセス財 ロデーブルを砂限してアクセスの金の実行可否を判定 し、前記プウセス財可デーブルにおいて財可設定のなされた処理のみを実行する構成を有することを将領とする</u>

(0014) さらに、本発明のデータ処理技団の一実施 顕様において、前記データで艦手段のデータ格所領域 は、各々が予め定められたデータ容量を持つ複数セクタ からなるブロックを複数有するフラッシュメモリであ り、前記プセス群型デーブルは、ブロック単位でのデ 一名の処理財団爆機を設定したデーブルとして構成さ 人。前記プレステーブルは、ブロック単位でのデ 一人は氏に観底されたプロック単位での処理財団爆構に 従って、プレルに関係されたプロック単位での処理財団爆構に 従って、プロック単位での処理財団爆構に 株式に、イスルースを構築とする。

独立ることを検索に立るで、 (0015) さらに、本発明のデータ処理技図の一葉縮 (0015) さらに、本発明のデータ処理技図の一葉縮 部からのアクセス命令に応じた処理が制記アクセス評可 デーブルにおいて許可数定のなされた処理範囲内である 場合にのみ、制記アクセス命令に応じた処理を実行し、 鎮アクセス命令に応じたメモリインタフェース内での処理成別に応じて処理成リフラグを設定し、前記制御制 は、前記メモリインタフェースにおける処理成別フラグ の設定の確認を条件として、制御部側の処理を実行する

構成を有することを特徴とする.

(0016)さらに、本発明のデータ処理装置の一実施 職様において、前記解的部は、和記アクセス命令がデー クフィイルの飲み出し処理である場合において、前記データ的アイルの野み出し処理である場合において、前記デーケルのリンス・イルのアドンプルのら膝み出し対象データファイルのアドレスを選択しが記火をリイングフェースに対しがおびに発力して表示・クランティルのアドレスに基づいて前記アクセス群コデーブルを動配は関連部から受信した能み出し対象データファイルのアドレスの設定された例域がデータファイルの下ドレスの設定された例域がデータがか出し可能 領域であるかるかを判定し、データ腺み出し可能 ある場合にのみデータ筋み出し処理を実行する構成を有することを格徴とする。

(0017) さらに、本発明のデータ処理装置の一葉簡単様において、前記前句話に、前記プクセス命令がデータファイルの音き込み処理である場合において、前記データ記憶手段内のデータ格納領集の母き込みアドスを選択し前記メモリインタフェースは、前記前母部から契信し、前記メモリインタフェースは、前記前母部から契信し、前記メモリインタフェースは、前記前母部から契信で、前記が主きを込みアドレスに基づいて前記アクセス許可デーブルを喚起して、第アドレスの設定された偶様がデーブルを参照して、数アドレスの設定された偶様がデーナーが音を込み可能関域であるか音がをからできている。

(0018) さらに、本発明のデータ処理装置の一葉筋 職様において、前記アクセス料のデーブルは、酸アクセ ス幹可テーブル内のデータで配の名無を食食するチェッ ク値として、酸テーブルカデータに基づいて生成される 改成チェック値(1CV)を付帯データとして有し、前 NI たもリインタフェースは、前記改算テェック値(1CV) NI た基づいて、前記のイス料可デーブルの改成チェックを実行する確号処理能を有し、前 があった、カーブルの改成チェックを表行する確号処理能を対し、 カ制記アクセス料可デーブルの改成チェックを実行する確号処理能を対し、 カ制記アクセス料可デーブルを決定・ リインタフェースに終定し、設定したアクセス料可デー ブルに従ったアクセス可否の判定に基づくデータ処理を 集行する構成を含することを特徴とする。

(0019) さらに、本発明のデータ処理接属の一実施 盤様において、前記アクセス幹司テーブルは、鍵プクセ ス幹司テーブル内のデータを強の有無を検査するチェッ り値として、数テーブル内データと、前記データ配筒平 段固有の類別・(1D)とを含むデークに基づいて生成 される改度チェック値(1CV)を付帯データとして有 し、前記メモリインタフェースによる前記法度チェック 値(1CV)に基づく検胚処理は、前記アクセス群司テーブルのデータ改度チェックに回え、鎖アクセス群司テーブルのデータ改度チェックに回え、鎖アクセス群司テーブルが正当なメディアに格納されているか否かの検距 処理として集行され、鍼検証により正当性の確認されたことを条件として、前記アクセス評司デーブルが正当なメディアに格納されているか否かの検距

インタフェースに設定し、設定したアクセス群ロテーブルに従ったアクセス可否の単底に基づくデータ処理を奨行する場底を指することを移設とする。

したことを条件として、前記データ配位手段のメモリに [0021] さらに、本発明のデータ処理装匠の一実施 単位でのデータ消去の可否、またはプロック単位でのデ 昨可テーブル中に設定されたプロック単位でのデータ指 去の可否、またはブロック単位でのデータ再生の可否の [0020] さらに、本発明のデータ処理装置の一装施 夕配位手段との相互認証処理を実行し、相互認証が成立 格納されたアクセス許可テーブルを前記メモリインタフ 塩体において、 前記データ 記憶手段は、 各々が予め定め プロックを複数有するデータ格納領域を持つフラッシュ 設定情報に従って、プロック単位での処理の可否を判定 られたデータ容量を持つ複数セクタを1プロックとした メモリであり、前記アクセス許可テーブルは、ブロック ルであり、前記メモリインタフェースは、前記アクセス **復様において、前記メモリインタフェースは、前記デー** エース内にセットする楜成を有することを特徴とする。 **--タ퍼生の可否の少なくともいずれかを設定したデー** する構成を有することを特徴とする。

(0022) さらに、本発明の第2の回回は、各々が予めためられたデータを留を持つ複数のセクタを1プロックとした複数プロックのデータ格納保険をおするデータ品数数面であり、前記データ格納保険のプロック単位でのデータ処理に似する評可認識を設定したアクセス評可デーブルを前記データ格制領域に格納したことを特徴とするデータ記数数図にある。

(0023) さらに、本売明のデータ配徴装置の一塊筋 職様において、前記アクセス許可テーブルは、前記データ格約領域における前記アクセス許可デーブルを格納したプロックに関するデータ処理許可能線を消去不可領域として設定した視成であることを特徴とする。

(0025)さらに、本発明の第3の側面は、データ船億年段に対するアクセスを実行するメモリインタフェースと、蚊メモリインタフェースの船卸を実行する側到卸とを有するデータ処理技匠におけるデータ処理方はつめ、前記メモリインタフェースは、前記データ総管年段内のデータも特領域に格許されたアクセス辞可テーブルをメモリインタフェース内にセットするステップと、前記が出まからの前記データ配管年段に対するアクセス命令に応じて、前記アクセス群可テーブルを参照してアクセス命令に表にし、前記アクセス群可テーブルを参照してアクセス命令の集行可否を判定するステップと、前記アクセス命令の集行可否を判定するステップと、前記アクセ

(0026)さらに、本発明のデータ処理方法の一実施 健様において、前記データ部施手段のデータ格物価様 は、各々が予め定められたデータ容量を持つ複数セクタ からなるプロックを複数布するフラッシュメモリであ り、前記アクセス幹可テーブルは、プロック単位でのデ ータの処理許可事様を設定したデーブルとして構成さ れ、前記メモリインタフェースは、前記アセス群可デ ーブル中に設定されたプロック単位での処理許可錯様に ・ブル中に設定されたプロック単位での処理許可錯様に (0027)さらに、本発明のデータ処理方法の一実施 臨様において、前記メモリインタフェースは、前記前数 能からのプクセス命令に応じた処理が前記アクセス許可 デーブルにおいて許可設定のなされた処理値面内である 場合にのみ、前記アクセス命令に応じた処理を実行し、 酸アクセス命令に応じたメモリインタフェース内での処 埋成功に応じて処理成功アラグを設定し、前記前卸部 は、前記メモリインタフェースにおける処理成功アラグ の設定の確認を条件として、前砂部側の処理を実行する ことを特徴とする。

(0028) さらに、本発明のデータ処理方法の一実施 臨場において、前記アクセス命令がデータル・カルの観 み出し処理である場合にもいて、前記所到部は、前記デ ータ記蔵手段内のデータ格特解域に対応して設定された フォイル部のデータ格特解域に対応して設定された フォイルのアドレスを選択し前記メモリインダフェースに送 信する処理を実行し、前記メモリインダフェースは、前 記刷的はから受信した説み出し対象データファイルのア ドレスに払去いて前記アクセス呼可テーブルを勢用 ドレスに対立いて前記アクセス呼可テーブルを終 ドレスに対立いて前記アクセス呼可テーブルを参加 で、 酸アドレスの製定された倒転がデータ課み出し可能 策略であるか否かを判定し、データ説み出し可能 第本であるをもでの。データ説み出し可能領域で ある場合にのみデータ観み出し回報解析で

(0029)さらに、本発明のデータ処理方法の一実施 態様において、前記プクセス命令がデータファイルの母 を込み処理である場合において、前記前御節は、前記デ ータ記憶手段内のデータ格納領集の皆き込みアドレスを 説状し前記メモリインタフェースに送信する処理を実行 し、前記メモリインタフェースに送信する処理を実行 し、前記メモリインタフェースに送信する処理を実行 レ、前記メモリインタフェースは、前記前側部から受信 トレ前記母を込みアドレスに基づいて前記プクセス許可 デーブルを参照して、歳アドレスの設定された領域がデ ータ母き込み可能領域である場合にのみデータ母き込み処理を 減行することを特徴とする。

ク値として、破ゲーブル内データに基づいて生成される 改復チェック値(ICV)を付帯データとして有し、前 記みモリインタフェースは、前記改置チェック値(IC V)に基づいて、前記フクセス群司デーブルの改置デェ ックを実行するステップと、前記プクセス群司デーブル の改復なしの判定が得られたことを発出して、前記プ か在入群コデーブルをメモリインタフェースに設定する ステップと、数定したフケセス群コデーブルで従ったア クセス可の音がに基づくデータ処理を実行するステップ プとを実行することを希徴とする。

**資様において、前記アクセス許可テーブルは、餃アクセ** ク値として、餃デーブル内データと、前配データ記憶手 し、前記メモリインタフェースは、前記アクセス許可テ メモリインタフェースに設定するステップと、設定した アクセス許可テーブルに従ったアクセス可否の判定に基 [0031] さらに、本発明のデータ処理方法の一実施 ス許可テーブル内のデータ改竄の有無を検査するチェッ **癸固有の駿別子(1D)とを含むデータに基づいて生成** される改竄チェック値(1CV)を付帯データとして有 **ーブルのデータ改竄チェックに加え、蹴アクセス許可テ ーブルが正当なメディアに格納されているか否かの検証** 処理として前配改成チェック値(1 C V)に基づく検証 処理を実行するステップと、該検証により正当性の確認 されたことを条件として、前記アクセス許可テーブルを **ゴくデータ処理を実行するステップと、を実行すること** を特徴とする。

(0032)さらに、本発明のデータ処理方法の一装施 磁様において、前記メモリインタフェースは、前記データ配金手段との相互移証処理を実行し、相互認証が成立したことを条件として、前記データ記憶手段のメモリに枯齢されたアクセス許可デーブルを前記メモリインタフェース内にセットすることを特徴とする。

(0033) さらに、本発明のデータ処理方法の一実施 環境において、前記データ記憶手段は、各々が予め定め られたデータを複数有するデータ格制領域を持つフラッシュ メモリであり、前記アクスが可テーブルは、ブロック 単位でのデータ消去の司名、またはブロック単位でのデ ・夕再生の司名の少なくともいずれかを設定したテーブ ルであり、前記メモリインタフェースは、前記アクセフ かであり、前記メモリインタフェースは、前記アクセフ がフランプルは、プロック がであり、前によびにカルクリーク がであり、前によびにフック単位でのデータ構 表の司名、またはブロック単位でのデータ 数定情報に従って、プロック単位での必要の可否を判定 することを構成とする。

(0034)さらに、本発明の第4の側面は、デーケ配 選手段に対するアクセスを集行するメモリインタフェー スと、験メモリインタフェースの創御を集行する創御部 とを有するデータ処理装置におけるデータ処理をコンピュータ・ンステム上で集行せしめるコンピュータ・プロ グラムを提供するプログラム提供媒体であって、前配コ

ンピュータ・プログラムは、前紀データ記憶事段内のデータ格納環域に格納されたプケセス許可テーブルをメモリインタフェース内にセットするステップと、前記術館館からの前記データ記憶事段に対するアクセス命令に応じて、前記アクセス許可デーブルを参照してアクセス許可デーブルにおいて野政定のなされた処理のみを実行するステップと、を有することを特徴とするプログラム提るステップと、を有することを特徴とするプログラム提

供媒体にある。 【0035】なお、本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実 行可能な汎用コンピュータ・システムに対して、コンピ ユータ・プログラムをコンピュータ可認な形式で提供す る媒体である。媒体は、CDやFD、MOなどの配路媒体 体、あるいは、ネットワークなどの伝送媒体など、その 形態は特に限定されない。 (0036) このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの撮船を実現するための、コンピュータ・プログラムを提供媒体との構造上又は協能上の路扇的図解を定義したものである。 換音すれば、競提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では路像的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

(0037)本発明のおらに他の目的、特徴や利点は、 後述する本発明の実施例や張付する図面に基づくより詳 題な説明によって明らかになるであろう。 (0038) (発明の実施の形態) [システム概要] 図1に本発明の データ処理装置の適用可能なコンテンツ配信シスチム相 成を示す。例えば音楽データ、回像データ、その他各種 プログラム等のコンデンツが、コンデンツ保持者または サーピスプロバイダのようなシステム運営者101か ら、インターネット等のネットワークを介して、または CD、DVD、フラッシュメモリを結撃したメモリカー ド等の各価記録媒体であるメディア103に結構され、 デバイス102に受信または送路されて再生、実行され る。デバイスは、例えばバーソナルコンピュータ (P C)、再生専用器、ゲーム器等のコンデンツ再性優能を 有するデバイスであり、例えば回像コンデンツ再生優能を もするデバイスであり、例えば回像コンデンツ再生優能を もするデバイスであり、例えば回像コンデンツを表示する。 (0039) このようなコンテンツ配信システムの構成中、コンテンツを再生するデバイスと、コンテンツを格辞、対対るメディイスと、コンデンツを格対なメディアとの評価格成を図2に示す。

[0040] 図2は、デバイス200、メディア1,210、メディア2,230の群題協院を示している。メディア1,210は、単稿なデーク戦み出し、曽倉込み処理のみをサポートする監督部を持つメディアであり、

等のデータ通信手段を介したデータ送受信処理を実行す る運信部201、各種指示を入力する入力部202、メ ポケーションリストを格納している内部メモリとしての イル制り当てデーブルによって管理され飲み出し可能な テンツの暗号処理を取行するコントローラを有するメデ イアである。メディア1, 210、メディア2, 230 [0041] 図2のデバイス200は、インターネット 3、これらの制御を実行する制御部205と、メディア とのデータ入出力処理のインタフェース機能を持つメモ リインタフェース (1/F) 邸300とを持つデバイス コントローサ 2 0 4、 さらに、 コンナンシのファイ 74録 メモリ部207を有する。なお、内部メモリ内に格納さ れるリポケーションリスト毎のデータファイルは、ファ メディア2,230は、メディアを鈎積するデバイスと の相互認証処理を実行し、またメディアに格納するコン と、不正なメディアやコンテンツの失効情報としてのリ の双方ともデバイス200に対する接着が可能である。 ッセージ、コンテンツ等の表示を実行する表示部20 指成や指し

(0042) デバイス200は、コンテンツの再生時に 再生対象のコンテンツがりポケーションリストに格納された失効メディア、失効コンテンツに対応していないことを確認した上で再生を行なう。再生対象のコンデンツがリポケーションリストにリストアップされていた場合は、再生処理が実行されない。リポケーションリスト、およびリポケーションリストを適用した再生処理にひいては後段で精細に説明する。

(0043) メディア1, 210は、データ入出力を順到する側割する側割を11と、コンテンツを格納するメモリ部212は、コンデンツを対象ペンを対応・ッダ情報ととに体納するのみならず、メディア国との国内の観別情報としてのメディア10、さらに、メモリアクセスコントロール情報を記述したアクセス終司デーブルであるBPT(Glock Permission Table)を格納ウー

でいる。

「でもり デバイス200のファイルシステムはメディアを関助した後に、アクセス昨可テーブルであるBPTをメディアから部み込み、メディアへ直接アクセスを行うメモリインターフェイス部300にBPTを応送し、管理させる。メモリインターフェイス部300にBPTを経過し、管理させる。メモリインターフェイス部300に、BPTを発電した後、受信したBPTについて改成チェック値(ICV)の検証を行う。ICVが正当なものと判断された場合のみ、BPTを有効なものとして保存する。メモリインターフェイス部300は、メディアのメモリにアクセスする命令を受信した時、このメディアのBPTに基づいたアクセスのみ実行する。BPTの場成、およびBPTを用いた処理に関しては後段で詳細にあ、およびBPTを用いた処理に関しては後段で詳細に

脱明する。 【0045】メディア2,230は、コントローラ23 1と、メモリ部232によって構成され、メモリ部23

認証処理あるいはコンテンツの暗号化、彼号処理を実行 し、レジスタを頒えた暗号処理部236、そして、これ ア21口、相互認証処理に適用する認証鍵Kake、コ ンテンツのメモリ 郎232への保存時の暗号 難である保 コンテンツを対応ヘッダ情報とともに格納し、さ らにアクセス許可テーブルであるBPT (Block Permis メモリ部232に対するデータ格納、またはデータ税み 存盤KSLO、さらに届号化対象の轍を隔号化する時の (1/F) 郜234、メデイアの렇別アとしてのメディ 初期値IV\_keys毎を格納した内部メモリ235、 sion Table) を格納している。コントローラ231は、 出し用インタフェースとしてのメモリインタフェース

格納倘成老因3 仁示寸。 メモリ部は例えば、EEPRO M (Electrically Erasable Programmable ROM)と呼ばれ るフラッシュメモリであり、プロック単位の一括消去方 [0046] [メディア内メモリ構成] 次に、メディア る電気的に昏き換え可能な不煩発性メモリの一形態であ 1, 210、メディア2, 230の各メモリ部のデータ 式によるデータ消去が英行される。

を含むデータ部と、エラー町正コード等の冗長データを 含む冗異部によって構成される。後段で詳細に説明する (1/F) 部300において発行される主なコマンドに が、冗長部には各セクタのデータ部内のセクタデータ改 [0048] [主要コマンド] 次に図2のデバイス20 [0047] 図3 (a) に示すように、フラッシュメモ リは、第1~Nまでの複数プロックを有し、各プロック って梅成され、各セクタは (c) に示すように実データ 位チェック値としてのICVが格納される場合がある。 は、(b)に示すように第1~Mまでの複数セクタによ 0において、制御部205と、メモリインタフェース ついて説明する。

[0049] まず、慰御郡205からメモリインターフ エイス (1/F) 部300に対するコマンドには、以下

フェイス (1/F) 部300は、ステータスレジスタの 現在のメモリインタフェース内のステータスを設定した ステータスレジスタの状態の既み出し。メモリインター ・ステータス銃み出しコマンド

指定したセクタのデータ説み出し処理命令。 ・セクタ航み出しコマンド

指定したセクタへのデータ省き込み処理命令。 ・セクタ笛き込みコマンド

セットされたヘッダの情報を元に、指定されたセクタの **昨母化データを復号して読み出す処理の実行命令。** ・セクタ復号航み出しコマンド

セットされたヘッダの情報を元に、指定されたセクタヘ

・セクタ商母智を込みコマンド

データを暗号化して皆き込む処理の実行命令。

旨定されたパラメータを元にヘッダを生成する処理の実 ヘッダ生成コマンド

**ヽッダをメモリーインターフェイス内にセットする処理** ヘッダセットコマンド

BPTセットコマンド

B P T をメモリーインターフェイス内にセットする処理

リポケーションリスト (Revocation List) セットコ

**不正メディア、不正コンテンツのリストであるリポケー** ションリスト (Revocation List) をメモリーインター

ら各部の制卸を実行する側御部233とを有する。

・更新用リポケーションリスト (Revocation List) チ フェイス内にセットする処理の実行命令。

更新用リポケーションリスト (Revocation List) に現 エックコマンド

在のリポケーションリスト (Revocation List) を更新 してよいかチェックする処理の実行命令。 ・メディア 1 認識コマンド

D)を読み出して、その1Dが有効かどうかチェックす 接続されたメディア 1 に対してメディアの駿別子(1 る処理の実行命令。

·の職別子(1D)が有効かどうかチェックする処理の 接続されたメディア2に対して相互認証をして、メディ メディア 2 認識コマンド 实行命令.

メモリ内のファイル割り当てテーブルを読み出す処理の ファイル割り当てテーブル呼び出しコマンド 实行命令.

メモリへのファイル割り当てテーブルを更新する処理の ファイル割り当てテーブル更新コマンド 與行命令。

[0050] メモリインターフェイス (1/F) 結30 0からメディア1に対するコマンドは、以下のものがあ

・1 口能を出しコレンド

F) 部300の詳細構成を図4に示す。各構成部の機能 【0051】 [デバイス内メモリインタフェース群描結 成] 次にデバイス 2 0 0 のメモリインタフェース(1 / メディア1の持つ10を読み出す処理の実行命令。

**ジスタである。ステータスレジスタ301の構成例を図** メモリインターフェイスの内部ステータスを保存するレ [0052]・ステータスレジスタ301 5に示す。各ビットは以下の意味を持つ。

メモリインターフェイスが内部処理をしているかの判別 y), 0:符優 (ready)) 用ビットである。

・ピット0 (bil 0) :ピジーンツグ

メモリからデータの銃み出しが広功したかの判別用ビッ ピット 1 (bit 1) : 観み出し成功フラグ (1:成功 (success), 0:失敗 (fail))

メモリヘデータの智き込みが成功したかの判別用ピット ピット2 (bil 2): 智者込み成功フラグ (1: 成功 (success), 0:失敗 (fail))

Ë ·ピット3 (bil 3) :メディア1セットフラグ セット (sei), 0: 未セット (nol sei))

接続されたメディア 1 が利用可能かの判別用ビットであ

接続されたメディア 2 が利用可能かの判別用ビットであ Ë ・ビット4 (bil 4):メディア2セットフラグ セット (sel) , 0: 未セット (nol sel) )

按続されたメディア 1 の駿別子(1 口)が、リポケーシ ヨンリスト (Revocation List) 内のリポーク (排除) 公 (OX), 0: 無効 (NG))

(]: 有 ・ピット6(bi1 6):メディア2有効フラグ メディア対象外かの判別用ビットである。 効 (OX), 0: 無効 (NG))

接続されたメディア2の職別子 (1D) が、リポケーシ ョンリスト (Revocation List) 内のリポーク (排除) ・ビット7(bil 7): ヘッダセット成功フラグ (): メディア対象外かの判別用ビットである。 成功 (success), 0:失敗 (fail))

・ピット8 (bi18):ヘッダ生成成功フラグ (1: 成功 ヘッダがメモリインターフェイス内にセット出来たかの 判別用ビットである。

(success), 0:失败(fail))

・ビット9 (bil 9) :リポケーションリスト (Revocati on List) セットフラグ (1: セット (sel), 0: 朱七 ヘッダの生成が成功したかの判別用ビットである。 ット (nol sel) )

ンターフェイス内にセット出来たかの判別用ビットであ リポケーションリスト (Revocation List) がメモリイ

·ビット10 (bit 10):更新用リポケーションリスト 更新用リポケーションリスト (Revocation List) が有 (Revocation List) 有効フラグ (1: 有効 (OX) , 0:

ソタフェース (1/F) 都300のステータス情報を保 (0053) ステータスレジスタ301は、これらのイ **効であるかどうかの判別用ビットである。** 

[0054] 図4に戻り、各構成の機能について説明を

**一夕の飢み寄きは、アドレスレジスタに飲み母きを肌始** するセクタアドレスを設定し、カウントレジスタに説み [0055] なお、外部メモリ、内部メモリに対するデ **碧きをする総セクタ数を設定し、コマンドレジスタにセ** クタ飲み告きコマンドをセットすることで実行される。 制御部より送信されたコマンドを保存するレジスタ [0056]・コントロールレジスタ305 データの全転送セクタ数を散定するレジスタ データの転送開始セクタを設定するレジスタ ・カウントレジスタ304

各種レジスタおよび送受信パッファなど、メモリインタ メモリインターフェイスの動作を設定するレジスタ -フェイスの制御を行う。 · 送受信仰御都306

送値データを格納するパッファ ・受信パッファメモリ308 ・送信パッファメモリ307

二

・ピット5 (bit 5) :メディア 1有効フラグ

**英信データを格納するパッファ** 

・送信レジスタ309

送個パッファメモリ307内のデータを送信するための

受信したデータを保存し受信パッファメモリ308に伝 ・受信レジスタ310 送するためのレジスタ

送個パッファメモリ307、受個パッファメモリ308 内のデータに対して、各価商号処理を施す。 [0057]·暗号処理部320 ・メモリ部321

ト、ブロック・バーミッション・テーブル (BPT) そ 場合、送受信仰到部306が側御部からのメディア認識 コマンド、あるいは外部メモリに対するデータの説み哲 ト、外部メモリから競み込まれるアクセス許可テーブル T)を格納、保存する領域である。リポケーションリス きコマンド等を受信した場合、セットされたりポケーシ ョンリスト、ブロック・バーミッション・テーブル (B PT)を参照した処理が実行される。これらの処理につ れぞれがメモリインタフェース内に有効にセットされた よび内部メモリから競み込まれるリポケーションリス としてのブロック・バーミッション・デーブル (BP 商号処理部320における暗号処理に必要な勉増瓶、 いては、後段でフローを用いて辞却に説明する。

[0058] さらに、メモリ都321には、暗号処理に まれる配送盤。コンテンツICV生成盤Kiev\_cont、コ Kdist:メディア2に右衽されるコンテンシ以外のコン テンツのセキュリテイヘッダ(Securily Header)に含 必要な整情報としては、以下のデータが格納される。

| CVを生成する際に用いるセキュリティヘッダ | CV Kicv\_sh:セキュリテイヘッダ (Securily Header) の

9

コマンドレジスタ302

CVを生成する際に用いる初期値(IV:Inilial Yalu 1 Vsh: セキュリテイヘッダ (Security-Header) の1

M.K.ake:相互認証用のマスター麭。

1 Vake:相互認証用の鮑の生成処理に適用するための 初期值 (1V:InitialValue).

1 Vaulh: 相互認証時のデータ生成用の初期値(1 V:1 nitial Yalue),

MKicv\_rl: リポケーションリスト (Revocation Lis 1) の1 CV勉を生成するマスター塾。

1) の1 CV盤を生成する時の初期値(IV:Initial V I Vicv\_r1 : リポケーションリスト (Revocation Lis

I Vrl: リポケーションリスト (Revocation List) の I CV生成時に用いる初期値(I V:Initial Yalu alue).

MKicv\_bpl:アクセス許可情報であるBPT(Block Pe I Vicv\_bpl: アクセス許可情報であるBPT (Block P 1 V\_keys:メディア2で、コンテンツ店も化用の額を店 ermission Table)のJ CV敷を生成する時のJ CV生 rmission Table) の1CV鉋を生成するマスター麭。 号化する時の初期値(1V:Inilial Yalue)。

わない。

1 Vbpl:アクセス許可情報であるBPT(Block Permi ssion Table) の初期値 (1 V: Initial Value). 成時に用いる初期値(IV:Inilial Value)。

[0060]・外部メモリ入出カインターフェイス32 送信レジスタ309、受信レジスタ310にあるデータ について、ECCチェックを行う専用プロックである。 (0059)·ECC回路323

外部メモリ(メディア 1, 2) に対する入出カインター フェイス。外部メモリとしては例えばフラッシュメモリ およびコンテンツ記録再生に伴うヘッダ情報、さらにブ ロック・パーミッション・テーブル (BPT) がこの外 部メモリス出カインターフェイスを介して入出力する。 を搭載したメモリカード箏がある。例えばコンテンツ、 ・内部メモリ入出カインターフェイス325 フェースを介して、内部メモリに格納された例えばリポ (0061) 外部メモリ入出カインターフェイス32 ケーションリストの入出力が実行される。

内部メモリに対する入出カインターフェイス。当インタ

4、および内部メモリ入出カインターフェイス325か らは、処理に応じて以下の各値号が外部メモリ(メディ ブ1,2),あるいは内部メモリに対して出力される。

CLE:コマンドラッチイネーブル ALE:アドレスラッチイネーブル CE:チップイネーブル

WE:ライトイネーブル RE:リードイネーブル

また、外部メモリ(メディア 1, 2) 、あるいは内部メ モリからの信号として、

(外都メモリ (メディア1, WP:ライトプロテクト

RDY/BUSY:レディー・ピジー

これら各種信号が入力される。

ィアのフラッシュメモリに格納されるコンテンツ構成に 等、各コンデンツは、図6 (a) に示すように各種属性 【0062】 [メモリ格部コンテンツ構成] 次に、メデ ついて図 6 を用いて説明する。音楽データ、画像データ 箔粗からなるセキュリティヘッダと、実データ郜として

のコンアンツとによって構成される。

ように、フラッシュメモリはプロック単位で消去が実行 キュリティヘッダ部またはコンテンツ部を格納する形態 とし、一括した消去処理が許容される場合を除いて、異 されるので、1プロックには同一コンテンツに関するセ なるコンテンツを1つのプロックに格納する処理は行な (b) に示すように、複数コンテンツのセキュリティヘ ッダ部とコンテンツ部との各ペアを格納する。前述した [0063] メディアのフラッシュメモリは、図6

【0064】 [セキュリティヘッダ構成] セキュリティ ヘッダは、各コンテンツに対応する属性情報である。

キュリティヘッダのデータ構成を図りに示す。 各データ 【0065】・フォーマットパージョン (Format Versi 内容について説明する。

セキュリティヘッダ (Security Header) のフォーマッ

トバーションを示す。

ロンテンツの疑別子(10)を示す。 ・コンドンツID (Content 1D)

コンテンツの葡萄を示す。例えばメディア 1、またはメ ディア2に格納されたコンテンツ、あるいは放送コンテ ・コンテンツタイプ (Content Type)

コンテンツの属性、例えば音楽、画像等のデータである ·データタイプ (Dala Type)

コンデンツのコンテンツ盤 (Kc) を使った暗号化処理ア ・暗号アルゴリズム (Encryption Algorithm) か、プログラムであるか箏を示す。

ルゴリズムを示す。例えばDESによる暗号化であるか

トリブルDES (Triple-DES)によるか等を示す。

れたアルゴリズムに対応する暗号モードを示す。例えば 暦号化アルゴリズム(Encryplion Algorillm)で指定さ ECBモードかCBCモードか等を示す。 ・暗号化モード (Encryplion Mode)

[0066] ・ 晦号化フォーマットタイプ (Encryption

イブ2か、コンテンツ金体に対して1つのコンテンツ難 コンデンツの暗号化フォーマットを示す。タイプ1かタ

Kcで暗号化するタイプをタイプ1とし、コンテンツの セクタ毎に異なる鍵Ksec\_nを適用してコンテンツ の暗号化を行なう娘様をタイプ 2とする。

【0067】図8に各タイプの暗号化フォーマット構成 を示す。図8 (a) がタイプ1の暗号化フォーマットで 箱号化されたコンテンツのメモリ格的構成であり、

(b) がタイプ2の暗号化フォーマットで暗号化された コンテンツのメモリ格技権成である。

成、すなわちセクタ依存型暗号化処理である。例えば図 の毎号化盤としたKsec\_1が対応して設成され、も て、すべてKsec—1を適用した毎号化処理が紡され ちセクタ非依存型暗号化処理である。図8 (b) に示す タイプ2の暗号化フォーマットは、フラッシュメモリの mが適用されて暗号化されたコンテンツが格納された俳 て格納される。プラッシュメモリのセクタmでは、セク を用いて暗号化されてメモリに格納された構成、すなわ **合セクタ毎に異なるセクタ懲Ksec\_1~Ksec**─ 8 (b) のフラッシュメモリのセクタ1では、セクタ1 マットは、コンナンシがすべた 1 つのコンデンツ糖K c [0068]図8 (a) に示すタイプ1の時号化フォー クタ1に格納されるコンテンツは、各プロッグにおい

【0069】このように、本発明の構成においては、各 セクタ毎に異なる暗号化粒を適用したコンデンツの暗号 処理が適用される。さらに、各セクタ毎に異なる暗号化 数を適用した処理館様においても、1つのセクタに1つ の鍵を適用したシングルDESによる処理、1つのセク 各種の暗号化態様が適用可能である。これらの処理形態 【0070】図7に戻り、セキュリティヘッダの構成に タに複数の触を適用したトリブルDESによる処理等、 については、さらに後段で詳細に説明する。 されて格託される。

・暗号化フラグ (Encryption Flag) ついて説明を続ける。

ラグを持つ。例えば0:非暗号化セクタ、1:暗号化セ **グ。ブロック内のセクタ数(例えば32セクタ)分のフ** クタ。なお、本例では1プロックを32セクタとする。 プロック内の各セクタの暗号化・非暗号化を示すフラ [0071] · 1 C V フラグ (1CY Flag)

グ。ブロック内のセクタ数 (32セクタ) 分のフラグを持 【0072】・ 毎号化コンアンツ類(K c\_Encrypted 0 プロック内の各セクタの1 CV付加・非付加を示すフラ つ。例えば0:ICVなし、1:ICVあり

・ 届中代 I C V 生成数(Kicy\_conl\_encrypled) 暗母化されたコンテンツ鮑の格納ਿ域(32個)

商号化されたコンテンツの I C V 作成のための数の格柄

【0073】・有効リボケーションリストパージョン (Valid Revocation List version)

たデータの再生処理等、リポケーションリストの参照を [0074]・セキュリティヘッダ1CV (ICY of Sec 再生を昨可しない。なお、自己デバイスにおいて格納し コンテンツ再生の際に有効に適用されるリポケーション リスト (Revocation List) のパージョン。コンデンジ (RevocationList) のパージョンがこれより古い切合、 耳生の像に、セットされているリポケーションリスト 適用する必要がないコンテンツには0を設定する。

セキュリティヘッダ(Securily Header)の改竄チエッ ク値 (1CV)。 urily Reader)

ディアやコンテンツの失効情報としてのリポケーション [0075] [リポケーションリスト] 次に、不正なメ リストの构成について説明する。 図9 にリポケーション リストの構成を示す。以下、各データについて説明す

【0076】・リポケーションリスト職別子 (Revocali on List 1D)

リポケーションリスト (Revocalion.List) 固有の識別 子としての10である。

> れ、セクタmに格納されるコンテンツは、各プロックに おいて、すべてKSec\_mを適用した唔号化処理が施

**グEの毎年化額としてKsec\_Eが対応して数値が** 

を示す。リポケーションリストは、更新され、更新時に 新たな不正なメディアやコンテンツの失効情報を追加す [0077]・リポケーションリストバージョン (Revo Jポケーションリスト (Revocalion List)のパージョン cation List Version)

**結果、リポケーションリストの更新を行わなければ、そ** ンツのヘッダ内に有効なリポケーションリストのパージ 古い場合には、コンテンツの肌み出しを中止する。その ョン情報を設定する。コンテンツ就み出しの際に、現在 デバイスに保持しているリポケーションリストのパージ ョンとコンデンツのヘッダ内にある有効なリポケーショ ンリストのパーションとを比較する。この協、現在保持 しているリポケーションリストのパーションの方がより 【0078】本発明の構成では、リポケーションリスト (Revocalion List)にパージョン位置を収定し、コンド のコンテンツの税み出しはできない。

トのパージョン情報と更新用のリポケーションリストの パージョン情報とを比較した、節ついりポケーションリ ストであると判断した時のみ、リポケーションリスト更 【0079】また、リポケーションリストの更新時にメ モリ・インターフェース部が現在のリポケーションリス 新を許可する構成とする。

ストの新旧比位処理、更新処理の具体的処理例について 【0080】パージョン信組を吊らたリポケーションリ は、処理フローを用いて後段で詳細に説明する。

[0081]・メディア11D数 (Number of Medial I

失効しているメディア」(Medial ID)の総数 ・メディア I I D(0) -メディア I I D(L - I) (Medial ID(0) - Medial ID(L-I)) 失効しているメディア I の機別子のリストである。

(0082)・メディア21D数 (Number of Media2)

失効しているメディア?(Media2 1D)の総数 ・メディア21D(0)-メディア21D(M-L) (Media21D(0)- Media21D(u-l)) 失効しているメディア2の雄別子のリストである。

(0083)・コンテンツID数(Number of Contents 1D) 失効しているコンテンツID(Contents 1D)の総数

矢別しているコンナンツェロー(Lontents ID) Owest ・コンテンツェロ (0) - コンテンツェロ (N-1) (Contents 10(0) - Contents <math>10(N-1) 朱鉛しているコンテンツ雑別子のリストである・(0.0.8.4]・リポケーションリストICV (10.9.8] evocation List)

リボケーションリストの改成チェック用のICV (0085)上述のように、本発明におけるリボケーションリストは、複数の極額(メディア、コンデンツ)の 総別子(1D)から協成される。このように、コンデンツやメディアの先効情報であるリボケーションリスト (Revosation List) に複数の面貌のリボーク対象 I A 北老れの偶るを真なる勢作として行うことによって、一つのリボケーションリストで複数のロンデンツ、メディーのリボケーションリストで複数のコンデンツ、メディアの地の様み出し時にメモリ・インターフェース部において、利用メディアまたは利用コンデンツの数別子(ID)と、リボケーションリストにリストされたID との風合を実行することにより、不正なメディアの使用や不正なコンデンツの鍵 【のの86】このようにコンテンツやメディアの複数の10を1つのリポケーションリストに設定した結成により1つのリポケーションリストで複数の極端のメディアとコンテンツのリポーク(排除)が可能になる。メディア経動時のリポケーションリストに基づくメディアの後据処理、コンデンツ処理時のコンテンツ後据処理の具体の処理については、後級で認明する。

(10年27) また、本税明の協成では、リボケーションリストは、外部メモリ等に直接アクセスするメモリインタフェースでセットアップされ、セットアップ後は、メデイアの総着時、コンデンツの両生時においてメモリインタフェースにおいて総様的に利用可能な構成としたので、コンデンツの利用時に繰り返し内部メモリから読み出すなどの処理が不要となり処理が効率的に実行され

(0088) [プロック・パーミッション・デーブル

をセットすることで、デバイスの制御部がいかなるプロ イルシステムが眺みとって暫き換えることによって、記 [0089] 本発明のデータ処理装置において採用され デバイスにおける音き替えを禁止したプロックに格納さ れるメディア自身のアクセス許可テーブルである。デバ **グラムを実行中でも、メディアのアクセス許可デーブル** に設定された許可情報に従ったメモリアクセスが行われ 場合、PC内のOSのファイルシステムが主体的に、記 ブルの内容を自由に告き換えが出来た。その為に、春込 4.禁止を設定したアクセス情報デーブルを格納する配録 イスはBPTを格納したメディアを用いて、コンテンツ データ智き込み毎のデータ処理を実行する場合、メディ アに直接アクセスするデバイスのメモリインターフェイ 来、例えばPC等においてコンテンツの再生を実行する 母メディアに格納されているアクセス情報デーブル(例 **堕しており、ファイルシステムがそのアクセス情報テー** メディアがあっても、そのアクセス情報テーブルをファ ス部にブロック・パーミッション・デーブル (BPT) であるブロック・パーミッション・テーブル (BPT) (BPT)] 次に、アクセス許可テーブルとして使用さ れるブロック・パーミッション・テーブル (BPT:B) えば、File Allocation Table : FAT)を読み込んで笛 母メディア内のデータを告き換えられる可能性がある。 5プロック・パーミッション・デーブル (BPT) は、 ock Permission Table)の構成について説明する。従 る結成とした。

{0090} 図10にプロック・パーミッション・デー パル (BPT) の構成を示す。以下、各データについて

説明する。 【0091】・フォーマットバージョン(Formal Yersi BPT (Block Fermission Table) のフォーマットバージョンを示す。BPT自体にも、各種のフォーマットがあり、そのいずれであるかを疑別するデータである。

・B P T韓別子(BPT 1D) ブロック・バーミッション・テーブル(B P T:Block Permission Table)の韓別子(1 D)である。

・プロック数 (Number of Blocks) B P T (Block Permission Table) で扱うプロックの総数を示す。前述したように、フラッシュメモリはプロック毎の消去がなされる。B P T により管理されるプロック数を示している。 ・ブロック#1ーブロック#n許可フラグ(Block\_II -1n Permission Flag) 各ブロックのアクセス耐阻フラグを示している。例えば フラグののブロックは、消去不可ブロックであり、フラ グ1のブロックは消去回ブロックであることを示す。 ・B P T - I C V (ICV of RPT) B P T (Block Permission Table) の改竄チェック用の i C V マガネス

[0092] デバイスのファイルシステムはデバイスを B媒した後に、プロック・バーミッション・デーブル (BPT) を例えばフラッシュメモリを搭載したメモリ カード等のメディアから競み込み、メディアへ直接アク セスを行うメモリインターフェイス部にBPTを転送 し、そのメディアに対するアクセス群司デーブルとして 管理させる。メモリインターフェイス部は、アクセス群 可デーブルを受債しBPTをセット(ex. 図4に示す メモリ語321)する。メモリインターフェイスは、メ ディアのメモリにアクセスするの令を受信した時、この メディアのアクセスするのもを受信した時、この メディアのアクセスするのもを受信した時、この

(0093)プロック・パーミッション・テーブル(BPT)には、例えばメディアのフラッシュメモリの各プロック単位での許可された処理協様、具体的には例えば指表可ブロック、 海去不可ブロック、 あるいは再生可ブロック、 再生不可ブロック等の設定がなされている。 メモリインクフェースは、これらのBPT設定に従って処理の可否を決定する。これらの処理の詳細は、後段できらに詳細に説明する。

(0094)なお、プロック・パーミッション・デーブル(BPT)には、改盛防止のための改選チェック値1 CVが設定され、BPTのメモリインタフェースへのセット時には、1CVチェックが実行され、改置ありと判定された場合には、BPTのセット処理を実行しない。従って、不正なアクセス許可デーブルを作成して、使用することが防止される。BPTの1CVはメディアの類別子(1D)に基づいて生成する。そのために、他のメディアにフクセス許可デーブルをコピーしたとしてもそのメディアには保護を記い。1CVの生成については、 (0095)メディアは、その製造時にプロック・パーミッション・テーブル(BPT)をメモリ(ex.フラッシュメモリ)の所定プロックに管を込んで出荷する。この路、プロック・パーミッション・テーブル(BPT)を格的したメモリ内のプロックについては、プロック消去不可の設定をプロック・パーミッション・デーブル(BPT)に記述する。本発明のデバイスは、メディアに指的したデータ消去処理において、BPTを参照してBPTに関係では、指去可であるプロックのみの消去を実行する際にたメディアについては、BPTの将去、BPTの将去、カティアののでは、BPTを将して数をので、BPTを持てコックのみの消去を実行する特別にされる。メディア内の日子で利用したファイルの寄き込み、再生処理については後述する。

【0096】メディア(フラッシュメモリ部轄データ配録採本)の製造時におけるプロック・バーミッション・デーブル(BPT)の設定フローを、図11および図12に示す。ここでは、メディアとコマンド通信が行えるメディア体の語を選してメディア韓別子(1D)の生成

マンドを送って(S31)、あらかじめメディアに格柄 ローである。各処理について説明する。まず、まだ初期 数定が行われていないメディアに対し、1D競み出しコ は、BPTのIDと初期負IVicv\_bplの排他論理和 ロック・パーミッション・テーブル (BPT) の設定フ された10を受信 (532) すると、その10をベース i c v\_bplと、初期色:I V i c v\_bplと、B P T職別 子(10)に基づいて生成する。具体的には、1CV生 にマスター観:MKicv\_bolによるDESモードでの ディア 1のタイプにおけるメディア作成器が攻行するプ [0097] 図11は、相互認証処理優能を持たないメ とした1 CV生成盤Kicv\_blを生成 (S33) す 5。1 C V 生成魏K i c v \_ bpは、マスター敏:MK D'1 V i c v\_bpl) に払づいて生成される。式の意味 成解Kicv\_bpl=DES (E, MKicv\_bpl, I とBPTの音き込みが連続動作で行われるものとする。 **商号化処理を実行するという意味である。** 

(0098) 次に、BPTのもフィールドに必要なパヴメータを設定(S34)し、各パラメータが設定されたBPTに基づいてICVを生成(後述する図14の必成を適用)し(S35)、生成したICVをBPTのICVメールドに設定(S36)する。このようにして場所されたプロック・パーミッション・デーブル(BPT)をメディアIC毎を込む(S37)。なお、前述したようにBPTの曾含込みプロックは、BPTにおいて結本不可保解として設定されたプロックとよる。

(0099) 図12は、柏耳器配処理協能を持つメディアのタイプにおけるメディア作成器が実行するプロック・パーミッション・デーブル (BPT) の税定フローである。各処理について説明する。まず、まだ幼期設定が行われていないメディア2との相互限語処理はよびセッション絵の共有(これらの処理については、後述する図22の処理を影照)を実行する。

(0100) 相互移移もよび総共有処理が様子すると、メディア2に対し1D競み出しコマンドを送って (S41)、1Dを飲み出し、1Dをペースとした1CV生成 盤Kicv\_bolを生成 (S42) する。1CV生成総 Kicv\_bolは、マスクー総:MKicv\_bolと、初 期値:1Vicv\_bolと、BPT協別子 (1D)に払づいて生成する。具体的には、1CV生成総Kicv\_bolに出ていて生成。 MKicv\_bol、1D 1Vicv\_bol)に基づいて生成される。まの意味は、BPTの1Dと初類値 (1Vicv\_bol)の体色機理和にマスター総:MKicv\_bol)の体色機理和にマスターを:MKicv\_bol)の体色機理和にマスターを:MKicv\_bol)の体色機理和にマスターを:MKicv\_bol)を必要には、BPTの1

を投行するという意味である。 [0101) 太に、BPTの台フィールドに必要なバラメータを設定(S45) し、名バラメータが設定された メータを設定(S45) し、名バラメータが設定された BPTに結づいて I C V を生成(後述する図14の例成 を適用)し(S46)、生成した I C V をBPTの I C Vフィールドに設定(S47)する。このようにして例

(0102) 図13にプロック・バーミッション・デーツル (BPT) の具体的構成例を示す。図13の (a) はメディア1、メディアラッション・モリップロック が成であり、図13 (b) は、プロック・バーミッション・テーブル (BPT) である。プロック・バーミッション・BPT1D、プロック教に続いて、各プロックの 得去面 (1)、消去不可 (0) が投近記・発行にBPT)が出来ません。 ストリックの 付してソークの 付してプロックの 付してソーク が投近に AM のを指すす (1)、消去不可 (1)が投げまして対対に A アロック・バーミッション・がれたアーツタ (B) 13の のではブロック # 2) は、プロック・バーミッション・ディスによる消去を防止し、BPTの智度替えが無行されない協成を持つ。

(0103) なお、図13に示すプロック・パーミッション・テーブル (BPT) の協成例は、各プロックの消去可(1)、消去不可(0) のみが設定された協成であるが、消去処理のみのアクセス軒可を設定した協成ではなく、読み取り(再生) 許可、不許可を設定した協成としてもよい。例えば再生および消去不可(11)、再生もよび消去可(00)とした投定が可能である。 (0104) なお、図2に示したようにメディア2では

メディア内に側が割8231を持っており、プロック・バーミッション・デーブル(BPT)が設定済みかどうかの状態を保持することもでき、BPTが設定されているの状態で、デバイスからBPTの新たな母を込み命が未たしても、受け付けない場成として、BPTの再告き込みを防止する構成としてもよい。[0105]なお、上述の例におけるBPT母を込みは、メディアとコマンド強信が行えるメディア作成器を選して実行する構成について説明したが、この他、メディアへのBPTの音を込みは、単純なメモリライターで作成したBPTを直接書き込みば、単純なメモリライターで作成したBPTを直接書き込む構成としてもよい。ただし、この場合も、メモリのBPT格別ブロックは、プロック・バーミッション・デーブル(BPT)において消

本不可領域として設定する。
(0106) [改成チェック値 (1CV) による改数チェック (1CV) による改数チェック (1CV) にはおけい (cek Yalue) によるデータ改成チェック処理について説明する。本発明の相応において、改成チェック (1CV) は、データ記憶手段に格納されるコンテンツ、プロック・バーミッション・デーブル、リボケー・ランジ、「等に付加され、それそれのデータ改成チェック処理にあった。なお、コンデンツについての改成チェック値は、セクタデータ単位に付加可能な過減である。コン

ゲンツ、ゾロック・バーミッション・テーブル、リボケーシン、プロック・バーミッションリスト格に付加されたICV処理の具体的形態については、後段で認明する。

(0107) DES毎号処理協成を用いた改竄チェック 他(1CV) 生成的を図14に示す。図14の協成に示すように対象となる改竄チェックデータを掲成するメッセージを8パイト単位に分割(以下、分割されたメッセージを0、D1、D2、・・、Dn-1とする)する。改竄チェックデータは、例えばコンテンツ自体であったり、上述したアクセス解司テーブルであるBPTの協成データであったり、あるいはリポケーションリストの協成データである。 (0108]まず、初期値 (inilial Yalue (以下、1 Vとする)) とDOを排他的論理和する (その結果を1 Lとする)。次に、11をDES暗号化部に入れ、改竄 チェック値 (ICV) 生成鍵ド i c vを用いて暗号化する (出力をE1とする)。 続けて、E1およびD1を排他的論理和し、その出力12をDES暗号化部へ入れ、改弦チェック値 (ICV) 生成鍵ド i c vを用いて暗号化する (出力E2)。以下、これを繰り返し、全てのメッセーンに対して暗号化処理を簡す。段後に出てきたENをコンテンツチェック値ICV、とする。

(0109) 改重のないことが保証された例えばコンテンツ生成時に生成した正当な1CVと、新たにコンデンツに基づいて生成した1CV、とを比較して同一性が立
抵、すなわち1CV、=1CVでおれば入力メッセージ、例えばコンテンツ、BPT、あるいはリポケーションリストに改重のないことが保証され、1CV、≠1CVであれば改強があったと判定される。

[0110] ICVを使用したデータ改竄チェック処理 フローを図15に示す。まず、改竄チェックの対象データを抽出し(S11)、抽出したデータに基づいて例え ば図14のDES届号処理協成により1CV、を計算する(S12)。計算の結果、算出されたICV、を計算する(S12)。計算の結果、算出されたICV、とデータ内に格荷されたICVとを比較し(S13)、一致した場合は、データの改竄が無く正当なデータであると判定(S14からS15)され、不一数の場合は、データの改竄があると判定(S14からS16)される。

(0111] リポケーションリストの改竄チェック用の改竄チェック値 (1CV) 生成総K i c v \_ r l l i, 予めデバイスのメモリインシフェース部300のメモリ部321 (図4を設置) 内に格納されたリポケーションリスト (Revocation List) の1C V盤を生成するマスターは、 リポケーションリスト (Revocation List) の1C V鍵を生成する時の加料値: 1V ic v l i) の1C V鍵を生成する時の加料値: 1V ic v l i) の1C V鍵を生成する時の加料値: V ic v l i) と、リポケーションリスト・バージョン(Rersion)に基づいて生成する。具体的には、改竄チェック値(1CV)生成機K: c v r l = DES(E, MKiov\_r l, Version i Vicw\_r l) に基づいて生成される。前記式の選供は、

パーション (Version) と初期位 (1 Vicv\_II) の姉伯 論理和にマスター館: MKicv\_IIによるDESモードで の商号化処理を実行するという意味である。リボケーションリストの改度チェック値は、このようにして生成された I CV生成総Ki cv\_IIを適用して初期値 I Vr I (メモリ部321に格納)を用いて図15に示すICV生成協成によって実行される。

有の正当なBPT、すなわち他のメディアにコピーされ ゴいて生成される。前記式の章味は、BPTの1Dと初 hた1CV生成数Kicv\_botを適用して初期値IVbo V生成構成によって実行される。なお、BPTの付帯情 版として格納されるICVは、BPT内のデータとBP 丁を格納したメディアの職別子 (10)を含むデータに 基づいて生成される。従って、BPTのICVチェック は、BPTのデータ改竄の有無のみならず、メディア固 [0112] また、プロック・パーミッション・テープ ル(BPT)の改竄チェック用の改竄チェック値(1C cv\_bolによるDESモードでの暗号化処理を裏行すると いう意味である。プロック・パーミッション・テーブル (BPT) の改竄チェック値は、このようにして生成さ るBPT歳別子(1D)に基づいて生成する。具体的に 期値(I Vicv\_bpl)の排色路理和にマスター盤:MKi 1 (メモリ部321に格納)を用いて図15に示す1 C 魏:MKicr\_bplと、BPTのICV殻を生成する時の 初期位: 1 Vicv\_bplと、BPTの属性情報中に含まれ =DES (E, MKicv\_bpl, ID'IVicv\_bpl) に基 V) 生成離Kicv\_bptは、予めデバイスのメモリ は、改竄チェック値(1CV)生成鏈Kicv\_bpt インタフェース部300のメモリ部321 (図4参照) 内に格納されたBPTのICV鑵を生成するマスター たBPTでないことを検証する機能も兼ね備える。

[0113] また、コンテンツのセクタ単位の改置チェック用の改置チェック目(1CV)生成数Kicv\_contは、コンテンツのヘッグ(セキュリティ・ヘッグ)中に暗号化されて格的されており、必要に応じてメモリインタフェースの暗号処理部320(図4参照)において、また、メディア2との相互認証後に集行されるメディア2のコントローラ231で集行されるロESーCBCモードによる復号処理によって取得される。これらの処理についてはフローを用いた説明中で詳細に説明

(0114] このようなデータ改成チェックの結果、例えばリポケーションリストの改竄が明らかになれば、リポケーションリストの砂照が四に右づくコンテンツの用生等の処理を禁止し、また、アクセス許可テーブルである B P T に故づくメディアのデータに対するアクセスを禁止する処理を実行する。これらの処理については、後段で詳細に認明す行する。これらの処理については、後段で詳細に認明す

[0115] [データ航み出し、音を込み処理]以下、

本発明のデータ処理装置において、デバイスがメディブからのデータ競争出しを行なう場合の処理、およびデバイスがメディアに対してデータを格許する場合に実行される処理について影明する。。。

[0116] (デバイス起動時処理)まず、デバイスを起動させた場合における処理を図16を用いて説明する。図16は、左側に図2におけるデバイス2000側間部205の処理を示したものである。処理スタート時点でのメモリインタフェース部300処理を示したものである。処理スタート時点でのメモリインタフェース部300のステータスレジスタの状態は、ピジーフラグ:0(特徴)、リボケーションリストセットフラグ:0(特徴)、リボケーションリストセットフラグ:0(未セット)である。

[0117] まず、デバイスが起助すると、何即節は、内部メモリのファイル制り当てデーブル呼び出しコマンドをメモリインタフェース部に送信(S101)する。メモリインタフェース部は、デバイスの内部メモリに対してファイル制り当てデーブルを均配、で102)して、ファイル制り当てデーブルを均配、が102)して、ファイル制り当てデーブルを均配、イスのプクセス可能な内部メモリ、外部メモリに格幹されたデータ、例えば様々なコンデンツ、あるいほりがイスのテリ、ファイル名、機能をクタが対応付けられた権の表をリン・デバイスは、ファイル割り当てデーブルに、ディレクトリ・ファイル名、格納セクタが対応付けられた権の表をし、デバイスは、ファイル割り当てデーブルにあら、がはなを持つ。デバイスは、ファイル割り当てデーブルに基づいて、様々なファイルのフクセスを行なう。

(0119) 節動部は、内部メモリに格称されたデータに対応するフィル動り当てテーブルを受信(S104)すると、テーブルに基づいてリボケーションリストの飲み出し処理を実行(S105) し、リボケーションリストの大・カコマンドと、リボケーションリストをメモリイングフェースに送信(S106) する。リボケーションリストをメモリイングフェースに送信(S106) する。リボケーションリストのセット処理は、リボケーションリストがインシッとは、メディアからのコンデンツ競み出し処理等、コンデンが処理の係、リボケーションリストにリストアップされたコンデンツまたはメディア語別子との比較処理を異行する。これらの処理については後述する。

(0120) リボケーションリストのセットコマンドと、リボケーションリストを簡単部から受価(S107) すると、メモリイングフェースは、ステータスレジスタのビジーフラグを1(ビジー)にセット(S108)し、リボケーションリストの政府チェック用の政府チェック値(ICV)生成整Kic、一「も生成(S

(0121) リボケーションリストの改成テェック用の 収盤チェック也 (1CV) 生成総K i c v\_r l lは、予 めデバイス内に格耐されたリポケーションリスト (Revo calion List) の1 C V飽を生成するマスター鑑:MKi

(0122)次にメモリインタフェースは生成した改成 チェック値 (1CV) 生成総K i c v\_r l を用いてリ ボケーションリストの1CV' を生成し、予めリボケーションリストのに格納された正しい1CVとの照合処理 (1CV'=1CV?)を実行 (S110) する。な お、1CV'の生成処理は、前述の図14で説明したD ESモードに基づいて、初期値1Vrlを用い、生成した 改成チェック値 (1CV)生成数Kicv\_r lを適用 した処理によって行われる。

受信するとセットされたリポケーションリストのコンテ (0123) 1CV'=1CVである場合 (S111で Yes)は、リポケーションリストが改竄のない正当な ものであると判定され、コンテンツの就み出し処理等の **協に参照可能な状態にセットし、リポケーションリスト** メモリ(例えばメモリ部321(図4参照))に格納さ れ、例えば、送受信制御部306が制御部205(図2 砂瓜) からメディア認識コマンドを受信するとセットさ スに装着したメディアのメディア離別子との照合が実行 され、また、送受値制御部306が制御部205からコ ンテンツの飲み出し処理に伴うヘッダセットコマンドを ンツ韓別子と、魏み出し対象コンテンツのコンテンツ韓 る。リポケーションリストはメモリインタフェース内の れたリポケーションリストのメディア製別子と、デバイ セットフラグを1 (セット) にセット (S112) す 別子との風合が実行される。

(0124)このように、リボケーションリストは、外 能メモリ等に直接アクセスするメモリインタフェースに セットアップされ、セットアップ後は、メディアの基準 時、コンデンツの再生時においてメモリインダフェース において複雑的に利用可能な構成とされ、コンデンツの 利用時に繰り返し内能メモリから眺み出すなどの処理が 不要となり処理が効率的に実行される。

(0125) 図16のフローの観明を競ける。ICV・キ」CVである場合(S111でNo)は、リボケーションリストに改成めりと判定され、リストの参照処理に ねづくコンテンツ処理を禁止し処理を体づする。以上の処理の株でにより、ピジーフラグは0にセットされる。(0126) 一方、何句話処は、ステータス誌み出しコマンドをメモリインタフェースに送信(S114)し、ピジーフラグが0となったことを条件(S115)とし

てリポケーションリストセットフラグを保存(S116)する。保存されるリポケーションセットフラグは、リストの改竄が無いと判定された場合は、リストが有効にセットされたことを示す」、その他の場合は0となにセットされたことを示す」、その他の場合は0とな

モリインタフェースにセットし、BPTを参照したメモ ず、有効に利用可能なメディアであることが確認された ことを条件として、メディアに格納されたアクセス許可 テーブルであるBPT(Block Permission Table)をメ [0127] (メディア認識時処理) 次に、デバイスに したようにメディアには、デバイスとの相互認証処理を **奥行しないタイプのメディア1と、デバイスとの相互認** か、具体的にはリポケーションリストに不正メディアと しての登録がないかを確認する処理を実行し、装替メデ ィアがリポケーションリストにリストアップされておら メディア認識時に実行する処理について説明する。前述 **証処理を実行するタイプのメディア 3 とがある。デバイ** スは、それぞれのタイプがデバイスに装着されると、メ ディアを利用したコンテンツ処理を実行してよいか否 メディアが装着された場合のメディアの有効性確認等 リアクセスを可能とする処理を英行する。

(0128) まず、メディア1が接着された場合のメディアが超級処理について図18、図19を用いて眺明す

【0129】図18、図19においても左側に図2におけるデバイス200の向御師205の処理、右側にメモリインタフェース部300必程を示している。当フロー関始時点で、メモリインタフェース部300のステータスレジスタの状態は、ピジーフラグ:0(特線)、メディア1有効フラグ:0(無効)、メディア1セットフラグ:0(未セット)の状態である。

【0130】まず、制御的は、デバイスに装着されたメディアがメディア1であることを認識する(520

1)。メディア難別は予め設定されたメディア形状に基づく機械的情報あるいはデバイス、メディア間の通信情報に基づいて行われる。創創的がメディア1であることを認識すると簡創的は、メディア1段韓ロマンドをメモリインタフェースに送信する(S202)。

(0131] メモリインダフェースは、御母部からのメディア1認識コマンドを受信 (S203) すると、ステーダスレジスタのピジーフラグを1 (ビジー) に設定し (S204)、メディア1に対してメディア1の疑別デ(1D)の跳み出しコマンドを送信 (S205) し、受信 (S206) する。さらに、受信したメディア1の1 Dと、既にセットされているリボケーションリスト中のリボーク (排除)メディア1のリストンのは参照合を実行 (S207) する。リボケーションリストは、先の図り、クタフェースにセットアップされ、セットアップ後は、メディアの技塾時、コンテンツの再生時において後にはい

てメモリインタフェースにおいて継続的に利用可能とな

(0132) 受価1Dと一致する1Dがリスト中に存在しなかった場合は、装着メディア1はリポーク対象メディアではなく、有効に利用可能なメディアであると判定(S208においてN0)し、ステータスレジスタのメディア1有効フラグを1(有効)にセット(S209)し、ピジーフラグを0(特徴)にセット(S210)する。受価1Dと一致する1Dがリポケーションリスト中にあった場合(S208においてをs)は、装着メディアはリポーク対象メディアであり、有効に利用できないと判定し、ステップS209の有数フラグの有効化処理を実行セザステップS210でピジーフラグを0

(特徴) にセットして処理を終了する。 [0133] 一方、何句部は、ステップS211において、ステータス読み出しコマンドをメモリインタフェースに送信し、ピジーフラグが0 (特徴) になったことを確認 (S212) の後、メディアフラグ状態を確認して有効 (フラグ:1) である場合 (S213でYes) にのみ処理を続行し、無効 (フラグ:0) である場合 (S213でNo)は、処理を終了する。

(0134)次に、図19に組み、傾望部は、メディブ1に図するファイル動り当てデーブル呼び出しコマンドをメモリインタフェースに送信(S221)し、メモリインタフェースは、ファイル割り当てデーブルの結構されたセク観み出しコマンドをメディア1に送信(S22)し、ファイル割り当てデーブルをメディア1から発出し、ファイル割り当てデーブルをメディア1から発信し、値触部に送信(S223)する。

価能を持つ。

(0135) 制御部は、メディア1に格辞されたデータに対応するファイル割り当てテーブルを受信 (S224) すると、テーブルに基づいてブロック・バーミッション・テーブル(BPT) の餓み出し処理を実行 (S225) し、BPTのセットコマンドと、BPTをメモリインタフェースに送信 (S226) する。BPTのセット処理は、BPTが名かである場合にのみ実行され、BPTが出げるといきれると、メディアからのコンテンツ音を込み処理等、コンテンツ処理の係。BPTを概してフック毎の消去が可能か否かを判定する。異級のBPTのック毎の消去が可能か否かを判定する。異級のBPT。

[0136] ブロック・バーミッション・デーブル(BPT)のセットコマンドと、BPTを耐御部から受虐(S227)すると、メモリインタフェースは、ステータスレジスタのピジーフラグを1(ピジー)にセット(S228)し、BPTの改竄チェック用の改竄チェック値(ICV)生成製Kicv\_bptを生成(S22

【0137】BPTの改竄チェック用の改竄チェック値 (1CV)生成皴Kicv\_bptは、予めデバイス内 に枯枯されたBPTの1CV皴を生成するマスター鞭:

MKicv\_bolと、BPTのICV数を生成する時の初期 由: IVicv\_bolと、メディアIDに基づいて生成する。具体的には、改置チェック値(ICV)生成総Kicc cv\_bpt=DES(E, MKicv\_bol, メディア,I D'IVicv\_bol)に基づいて生成される。共の意味は、メディア IIDと初期値(IVicv\_bol)の排他協関和にマスター総:MKicv\_bollの特色協関和にマスター総:MKicv\_bolによるDESモードでの商争化処理を実行するという意味である。

(0138)次にメモリインタフェースは生成した改置チェック値(ICV)生成総Kicv\_botを用いてBPTのICV'を生成し、予めBPT内に格納された正しいICV値との照合処理(ICV'=ICV')を実行(S230)する。なお、ICV'の生成処理は、前端の図14で説明したDESモードに基づいて、切が値1か10年度は、生成した改成アェック値(ICV)を総Kicv\_botを適用した処理によって行われる。なも、BPTの付着機能として格納されたICVは、メディアのオを指揮をして格納されたICVは、メディアコンクは、BPTのデータに基づいて生成されてもか。ICVのチェックは、BTのデータは近の右線のみなってにと一されたBPTでないことの砂缸や鉄和のメディアにコピーされたBPTではないことの砂缸や鉄和値えるアにコピーされたBPTではないことの砂缸や鉄和面点を

(0139) 1 CV' = 1 C V である場合 (S 2 3 1 で Y e s) は、B P Tが正当なメディアに指幹された改竄のない正当なものであると判定され、コンデンツ処理等の協に参照可能な状態にセットし、メディア 1 セットフラグを1 (セット) にセット (S 2 3 3 2 プレン処理を禁止し処理を検了する。以上の処理の終了アンツ処理を禁止し処理を検了する。以上の処理の終了により、ピジーフラグは0にセット (S 2 3 3) され

[0140] 一方、何如郎師は、ステータス館み出しコマンドをメモリインタフェースに造傷(S234)し、ピジーフラグが0となったことを条件(S236でYes)としてメディア1セットフラグを保存(S236)する。保存されるメディア1セットフラグは、BPTの改竄が無いと判定された場合は、メディア1が有効にセットされたことを示す1、その他の場合は0となる。

[0141] 次にメディア2がデバイスに基格された際のメディア2碗路処理について、図20、図21を用いて設明する。メディア2は、図2を用いて設明したように、デバイスとの相互認証を集行するメディアである。[0142] 図20のステップS301からS304のステップは、メディア1の確認処理におけるステップS201~5204と同様であるので認明を金略する。

【0143】ステップS305において、メモリイングフェースは、メディア2との袖互関距処型を実行する。[0144] 図22に、共通穀略号方式を用いた袖互総距方法(180/16、9798-1)の処理シーケンスを示す。図

ESのCBCモードで鮑Kabを用いてデータを暗号化 通の秘密機、認証観である。DESのCBCモードを用 いた塾Kabによる晦号化処理は、例えばDESを用い **応号文E1を生成し、続けて暗号文E1とRbとを排他** て時号化し、暗号文臣2を生成し、さらに、暗号文臣2 と1D(b)とを排他的論理和し、DES俯号化部にお いて、処Kabを用いて略号化して生成した暗号文E3 に送信する。これを受信したAは、新たに64ピットの 乳数Raを生成し、Ra、Rb、ID(b)の順に、D し、Bに返送する。なお、犂Kabは、AおよびBに共 的論理和し、DES暗母化部において、蠍Kabを用い る。図22において、まず、Bが64ビットの乱数Rb を生成し、Rbおよび自己の1Dである1D(b)をA 2.2においては、共通処略号方式としてDESを用いて た処理においては、初期値とRaとを排他的論理和し、 DES暗号化部において、犂Kabを用いて暗号化し、 いるが、共通機略号方式であれば他の方式も可能であ

(0.145) これを受信した日は、受信データを、やはり共通の秘密数としてそれぞれの配録素子内に格納する数Kab (昭経数)で復号化する。受信データの復号化りが開始Kabで資号化し、初期也よ市他的諸理和し記数Raを得る。次に、確与文目を認確的に、その結果と目と基礎的結婚和し、10(b)を得る。成後に、確与文目を建建して、10(b)を得る。こうして得られた。10(b)を得る。こうして得られた。Rb にし、10(b)を得る。こうして得られた。Rb にりのうち、Rb および10(b)が、Bが送信したものと一致するか後私する。この後低に通った場合、BはAを正当なものとして認証する。この後低に通った場合、BはAを正当なものとして認証する。

とによって送信データ(Token-AB)を生成する。

-.(Kses)を追款によって生成する。そして、Rb、Ra、Ksesの刷に、DESのCBCモードで認在する。 Aに混送する。 (0147)これを受信した人は、受信データを認証・一Kakeでは合作である。 こうして得られたRb、Bの送号化処理の様である。こうして得られたRb、Ra、Ksesの内、Rb およびRaが、Aが送信したものと一致するか検証する。 互いに相手を認正した後には、セッションキーKsesは、認証後の結6週

[0146] 次にBは、認証後に使用するセッションキ

[0152] 次にメディア2コントローラは、認証後に

(0148)なお、受留データの検証の協に、不正、不一致が見つかった場合には、相互移証が失敗したものとして、その後の相互間のデータ通信処理が禁止される。(0149)図23、図24に本税明のデバイスとメディア間における相互移転、鍵(セッション線)共布処理フローを示す。図23、図24において、左側がデバイスのメモリインタフェース、右側がメディア2のコントローラにおける処理である。

a とを排他的論理和し、쇛Kakeを用いて暗号化して 暗号文E2を生成し、さらに、暗号文E2とメディア2 C暗号文E3を生成し(S406)、生成したデータE 1||E2||E3をメディア2コントローラに送信(S4 暗号化し、暗号文E1を生成し、続けて暗号文E1とR る認証勉生成用マスター数:MKakeを適用しDES fたに乱敷Rbを生成(S405)し、初期値1Ⅴ\_\_a I Dとを排他的論理和し、数Kakeを用いて暗号化し 【0150】まず、メディア2コントローラが乱数R a を生成(S401)し、Raおよび自己の1Dであるメ (S402) する。これを受信(S403) したデバイ utカとRbとを排他的論理和し、蛇Kakeを用いて 4) する。さらに、デバイスメモリインタフェースは、 スメモリインタフェースは、受信したメディア21D と、初期値(IV\_ake)の排他論理和に自己の所有す 商号化処理を行なって認証数Kakeを生成(S40 ディア 2 1 D をデバイス メモリインタフェースに送信 07) する。[11] は、データの結合を意味する。

a' およびメディア 2 1 D'が、送信データと不一致で あったときは、相互認証が失敗 (S413) したものと ントローラは、受価データを、認証轍Kakeで彼号化 メディア 2 はデパイスを正当なものとして認証する。R [0151] これを受信 (S408) したメディア 2コ 暗号文E 1を認証処Kakeで復号化し、初期値と排色 的論理和し乱数Rb、を得る。次に、暗号文E2を認証 し、Ra.を得る。最後に、暗号文E3を認証盤Kak **e で復号し、その結果とE2を排他的論理和し、メディ** (S410, S411) する。この検証に通った場合、 (S409) する。受信データの復号化方法は、まず、 ア210'を得る。こうして得られたRa'、Rb'、 数Kakeで彼号し、その結果とE1を排他的論理和 メディア210'のうち, Ra' およびメディア21 D'が、メディア 2 が送借したものと一致するか検証 し、その後のデータ通信を中止する。 使用するセッションキー (Kses) としての副数を生成 (S412) する。次に、図24のステップS421 において、Ra、Rb、Ksesの順に、DESのCB Cモードで昭延数Kakeを用いて暗号化し、デバイスメモリインタフェースに送信(S423) ウたデバイスメモリインタフェースに送信(S423) レたデバイスメモリインタフェースは、受信アータを認経数Kakeで領号(S424) する。こうして得られたRa"、R号(S424) する。こうして得られたRa"、R号(S424) する。こうして得られたRa"、R号(S424) する。こうして得られたRa"、R号(S424) する。こうして得られたRa"、R号(S424) する。こうして得られたRa"、R号(S424)する。こうして得られたRa"、R号(S424)を通過したもののと一致するが表情にある。

1、Ksesの内、Ra"およびRb"が、デバイスが送信したものと一致するか検証(S425, S426) する。この検証に置った場合、デバイスはメディアを正当なものとして認託(S427) する。互いに相手を認正した後には、センションキーKsesを共有等を認正した後には、センションキーKsesを共有(S429) し、認証後の総部通信のための共通験として利用される。Ra"およびRb"が、送信データと不て利用される。Ra"およびRb"が、送信データと不

一致であったときは、相互認証が失敗(S428)した ものとし、その後のデータ通信を中止する。

(0154) 図20に戻り、メディア2の認識処理について説明を続ける。ステップS305において上述の相互認証、盤共有処理が実行され、ステップS306で相互認証が成功したことが低認されると、相互認証処理時に受信したメディア2の1Dと、既にセットされているリボケーションリスト中のリボーク(体除)メディア2のリストとの比較照合を実行(S307)する。

(0155)受信1Dと一致する1Dがリスト中に存在しなかった場合は、装巻メディア2は以ボーク対象メディアではなく、有効に利用可能なメディアであると判定(5308にせいてNo)し、ステータスレジスタのメディア 2 有効フラグを1 (有効)にセット (5310)する。要値1Dと一致する1Dがリボケーションリストラ・受信1は一分数条メディアであり、有効に利用できないと判定し、ステップS309の有効フラグの有効に、処理を実行せずステップS310でビジーフラグを0(特機)にセットして処理を推了する。

(0156) 一方、耐却部は、ステップS311において、ステータス誌み出しコマンドをメモリインタフェースに送信し、ビジーフラグが0(特優)になったことを確認 (S312)の後、メディアフラグ状態を確認して有効 (フラグ:1)である場合 (S313でYes)にのみ処理を統行し、無効 (フラグ:0)である場合 (S313でYes)にのみ処理を統行し、無効 (フラグ:0)である場合 (S313でNo)は、処理を終了する。

[0157] 次に、図21に進み、配卸部は、メディア2に図するファイル型り当てデーブル呼び出しコマンドをメモリインクフェースに送信(S321)し、メモリイングフェースは、ファイル型り当てデーブルの格辞されたセク部み出しコマンドをメディア2に送信(S32)し、ファイル型り当てデーブルをメディア2から受信し、何知部に送信(S323)する。

(0158) 制御部は、メディア2に格納されたデータに対応するファイル制り当てテーブルを受信 (S323) すると、テーブルに基づいてブロック・バーミッション・テーブル (BPT) の総み出し処理を実行 (S325) し、BPTのセットコマンドと、BPTを大モリインタフェースに送信 (S326) する。BPTのセット処理は、BPTが有効である場合にのみ実行され、BPTがセットが理は、BPTが有効である場合にのみ実行され、BPTがセットされると、メディアからのコンデンツ管を込み処理等、コンデンツ処理の際、BPTを参照してブロック毎の消去が可能か否判にする。異像のBPTを参照したデータ音込み処理については、後段で説明を参照したデータ音込み処理については、後段で説明

【0 1 5 9】プロック・バーミッション・デーブル(B PT)のセットコマンドと、BPTを傾倒部から受信 (S 3 2 7)すると、メモリインタフェースは、ステー

タスレジスタのビジーフラグを1(ビジー)にセット (S328)し、BPTの設置チェック用の設成チェック値(ICV)生成観Kicv\_britを生成(S32 (0160) BPTの改成子エック用の改成チェック句 (1CV) 生成総Kicv\_bptは、予めデバイス的に格的された。BPTの1CV総を生成するマスター総: MKicv\_bptと、サディア21Dに基づいて生成する。具体的には、改成チェック値 (1CV) 生成総Kicv\_bpt, ディア21D1Vicv\_bpt)に基づいて生成するアイア21D1Vicv\_bpt)に基づいて生成するサイア21D2が開催(1Vicv\_bpt)の指向協議和にマスター総: MKicv\_bptiの非他協議和にマスター総: MKicv\_bptiの非他協議和にマスター総: MKicv\_bptiの非他協議和にマスター総: MKicv\_bptiによるDESモードでの情号化処理を実行するという意味である。

(0161) 次にメモリインタフェースは生成した改成 チェック位 (1CV) 生成総Kicv\_bplと1vbplを 用いてBPTの1CV'を生成し、予めBPT内に格材 された正しい1CV位との原合処理 (1CV'=1CV') を実行 (S330) する。なお、1CV'の生成処理は、前途の図14で設明したDESモードに払づいて、初期位1Vbplを用い、生成した改成チェック位 (1CV) 生成総Kicv\_bplを適用した処理によって行われる。なお、BPTの付券情報として格幹されたってりは、メディア21Dを含むデータに払づいて生成されており、1CVのチェックは、BPTのデータ改成の有無のみならず、メディア固ちの正当なBPT、すなわち値のメディアにコピーされたBPTでないことの数据 (0162)1CV'=1CVである場合(S331でYes)は、BPTが正当なメディアに格時された政的のない正当なものであると判定され、コンデンツ処国等の場に参照可能な状態にセットし、メディア2セットフラグを1(セット)にセット(S332)する。1CV'=1CVである場合(S331でNo)は、BPTに改成ありと判定され、BPTの砂原処型に払づくコンデンツ処理を禁止し処理を終了する。以上の処理の終了により、ピジーフラグは0にセット(S333)され

も兼ね備える機能を持つ。

ットされたにとを示す1、その他の場合は0となる。[0164] (データファイル院み出し処型)次に、データファイル院み出し処型。次に、データファイルの説み出し処型について図25のフローを用いて設明する。データファイルには、音楽データ、回像データ毎のコンテンツデータファイル、さらに前送り

(0165) まず、傾仰部は、ファイル割り当てデーブル (図17巻照) から観み出し対象データのセクタアドレス (S (1) ~S (k)) を取得 (S501) し、メモリインタフェースに取得したセクタS (i) 観み出しコマンドを顧及送信 (S502, S503) する。メモリインタフェースは、セクタS (i) 観み出しコマンドを受信 (S504) すると、ピジーフラグを1 (ビジー) に設定 (S505) し、受信セクタS (i) が内部

メモリか、外部メモリであるかを制定(S506)し、 外部メモリである場合は、メディア1かメディア2のセットフラグが1(メディアが有効にセットされているこ とを示す)であるかを制定(S507)し、セットフラ グが1である場合には、さらにプロックバーミッション デーブル (BPT) を修照して、BPTが館み出し対 象であるセクタS (i) を題み出し終可対象プロックと して設定しているかを判定(S508)する。BPTに 観み出し終可プロックの設定がある場合には、外部メモ 切から該当セクタのデータを眺み出す(S509)。

(0166)なお、数み出し対象データがBPTによる管理のなされていない内部メモリ内のデータである場合は、ステップS507、S508はスキップする、ステップS507、S508はスキップする、ステップS67、S508の判定がNoである場合、すなかもともなる。(1)を結れてない場合、または、BPTにセクタS(1)の数か出し断可必要定されていない場合には、ステップSが10ではからであり、数み出しエラーとして観み出し成りフラグが0にでいっされる。

(9167) ステップS506~S508の判定プロックにおいて、対象セクS(i)の就み出しが繋行司と判定されると、メモリから験当セクタが認み出され、セクタに対応して設定されている元長部の縣り訂正符号に ねづく帳り訂正処望が実行 (S510) され、以り訂正符号にが成りした (S511) ことを確認し、就み出し成功フラグを1(成功)にセットし、説み出し結果をパッファに枯枯 (S512)し、ピジーフラグを0(特線)に設定 (S513) して処理を終了する。

(0168)また、耐御館は、ステップS515~S520において、メモリインタフェースのステータスを踏み出して、ピシーフラグが0の状態において、競み出し成功フラグが1であることを条件として誘み出しデータをパッファから取り出して保存し、アドレスを超太インクリメントして、データを簡次パッファから取り出して、

R存する処理を載り返し実行し、すべての認み出し対象 セクタを保存した後、全額み出しセクタデータからファ イルを構成して処理を終了する。

[0169] (ファイル毎を込み処理)次に、データファイルの毎を込み処理について図26のフローを用いて説明する。図26に示すフローは、内部メモリ、外部メモリ(メディア1、メディア2)のいずれかにファイルを皆を込む際の共通処理フローである。図26において、左側がデバイスの耐御紙、右側がデバイスのメモリインタフェースの処理である。

[0170] まず、何望部は、毎き込み対象フィルをセクタに分割する。分割されたデータをD(1)~D(k)とする。何望部は、次に各データD(i)の容さ込みセクタS(i)を設定して、メモリイングフェースにセクタS(i) 容容込みコマンドと、データD(i)を確決送電(S602~S604)する。メモリイングフェースは、セクタS(i) 哲き込みコマンドを受信(S005)すると、ビジーフラグを1(ビジー)に数

定 (S 6 0 6) し、受信セクタ (i) が内部メモリか、外部メモリであるかを判定 (S 6 0 7) し、外部メモリである始合は、メディア 1かメディア2のセットフラが1 (メディアが有効にセットされていることを示す) であるかを判定 (S 0 0 8) し、セットフラグが1 である場合には、さらにプロックパーミッション・デーブル (B P T) を参照して、B P Tが智章込み対象であるセクタ (I) を母側には、B P Tに留き込みが高くして設定しているかを判定(S 6 0 9) する。B P Tに留き込みが1フックの設定がある場合には、セクチに対応して設定する関り正正な号を生成(S 6 1 0) し、セクタ S (i) にデータ D (i) と関り訂正符号を持つ元長部を智章込み、留き込み成功フラグを I (成功)にセットし、ビジーフラグを 0 (特徴)に設定(S 6 1 4) す

スチムを持つようなシスチムの場合にはファイルシステ

ム自体に大幅な変更を必要とする。

(0171)なお、毎き込み対象データがBPTによる 管理のなされていない内部メモリ内への毎き込み処理である場合は、ステップS608、S609はスキップする。ステップS608、S609的にがNoである場合、すなわちメディアのセットフラがNoである場合、すなに、BPTにセクタS(i)の母き込み評可が設定されていない場合には、ステップS613に適み、母き込みエラーとして母き込み成功フラグを0にセットする (0172) また、粉御部は、ステップS616~S620において、メモリインタフェースのステーケスを飲み出して、ピジーフラグが0の状態において、曾老込み成功フラグが1であることを象件としてアドレスを隠水インクリメントして、曽舎込みデータを確水メモリインタフェースに送信する。すべての処理が終了すると、ファイル制り当てテーブルの更新処理を実行(S621)し、更新したファイル制り当てテーブルを更新コマンド

が必要となるためヘッダのサイズが膨大になってしまい タ部分にそのセクタを暗号化するための穀を格納する方 塾の寅 なにはデータを殴けなくなるためデータサイズが **回該りしたしまうにとと、ガー、巵御部回たファイルツ** るためにコンテンツ部に対する暗号化を行う場合がある セクタの数だけ8パイト (DESの場合) または16パ イト(トリブルDES(Triple-DESの場合))の総情報 **母られたメモリ領域のデータ領域を減少させてしまうこ** メモリインタフェースはコマンドに従ってファイル勧り [0173] [セクタ位配に応じた皓号化雑を適用した **時号化処理] 次に、セクタ位置に応じた時号化鍵を適用** した時号化処理について説明する。 著作権などを保護す が、コンテンツ部全体に対して一つの暗号化盤を使って し、攻撃が容易となってしまう危険性がある。通常はコ ンテンツ部をできるだけ分割し、それぞれを異なる蠍で 暗号化する方が望ましいと言える。 本システムでのコン 当てテーブルの書き込み処理を実行(S623)する。 とになり、実用上好ましくない。また、各セクタのデー 法をとればヘッダサイズに影響を及ぼすことはないが、 が、ヘッダ領域に鍵を保存するという目的の場合には、 とともにメモリインタフェースに送信(S622)し、 暗号化すると、同一の塾の元での大量の暗号文が発生 テンツ暗号化の最小単位として、セクタが挙げられる

(0174] そこで、本発明のシステムでは、先に説明した各コンテンツの属性情報であるセキュリティヘッグ
 (図74周) の中に例えば、メディアの1ブロックもたりのセクをMに対応するM個の整備報を結構し、これちをセクタに対する時毎化線として適用する(図8時間)。図7に示したセキュリティヘッダ中のKc\_Bintypied31が32個の時毎に終Kcがを示す。なお、[Encrypted31が32個の時毎代数Kcが時時代されて格約年度にいったことを示す。これらの複数の時のさセクタのブロック特位図によって線を選択してセクタ対応の暗号化線として用いる構成とした。

(0175)図27に、コンチンツのヘッダ指揮としてコンテンツに対応して生成されるセキュリティヘッダにおける総格的協成と、合格が総と、合線の適用対象となるメモリ内の合セクタとの対応を説明する図を示す。図27(a)が先回で着いて説明したセキュリティッグ内の総格的組を信略化して示した図である。図27(a)のセキュリティヘッダには、Kc(0)~Kc(N-1)までのM圏の総(コンテンツキー)が特的されている。ヘッダには緩歩がにおいて・ジャー)が特別を打ている。ヘッダには緩歩がにおけ、さらにヘッダ情報の減減チェック用の1CVが結構されている。

(0176) このM個のコンテンツキーは、例えば図27(b) に示すように各々が各セクタに対応付けられて各センタに結構する下で各センタには開される。先に各センタに格納するデータの暗号化に使用される。先に

図3を用いて説明したように、プロック単位での指去を行なうフラッシュメモリは、図27 (b) に示すようにデータ格的領域がプロック単位に分割され、各プロックはさらに視数セクタに分割されている。例えば鍵K。(0) を、メモリの各プロックのセクタのに格群するデータの暗号化鍵として適用し、鍵K (s) を、メモリの各プロックのセクタ sに格群するデータの原母化鍵とす。 きらに、鍵K (M-1) を、メモリの各プロックのセクタ sに格群するデータの原母化粒とす。 まらに、鍵K (M-1) を、メモリの各プロックのセクタ m-1に格群するデータの原母化鍵とす。

(0177) このように、セクタに対応して現なる暗母 鍵を適用してデータを格的することにより格所データ (ex. コンデンツ) のセキュリティが高められる。す なわち、コンデンツ金体を1つの敵で暗母化した場合 は、 酸剤型によるコンデンツ条体の質や可能化なる に対し、本稿成によれば、1つの数の類型によってデー 実体を質母することは不可能であるからである。 (0178) 時号化プルゴリズムは、例えば1つの時号 総によるDES 時号化処理を抜行するシングルDESが 適用される。また、シングルDESではなく、時号化に 2つ以上の鍵を使用するトリブルDESではなく、時号化に 2つ以上の鍵を使用するトリブルDESではなく、時号化に 2つ以上の鍵を使用するトリブルDESではなく、時号化に 2)を適用した暗号化構成としてもよい。

(0179) トリブルDES (Triple DES) の辞制 体成的を図28に示す。図28 (a), (b) に示すよ うにトリブルDES (Triple DES) としての他成に は、代数的には以下のような2つの現なる顕緑がある。 図28 (a) は、2つの命号線を用いた例を示すもので あり、鏡1による時号化処型。鏡2による位号化処型。 さらに鏡1による時号化処型の顔に処理を行う。鏡は、 K1、K2、K1の樋に2面線用いる。図28 (b) は 3つの命号線を用いた例を示すものであり、鏡1による 暗号化処理。鏡2による毎号化処理、さらに鏡3による 暗号化処理の顔に処理を行い3回とも暗号化処理を行う。 続1、K1、K2、K3の頃に3値鏡26行う。 をこのように放数の処理を通ばさせる場成とすること。 スングルDESには成してセキュリティ路度を向上

させることが可能である。 【0180】図29に、メモリに格納するデータの各セクタ体に異なる2つの略号観のペアを適用してトリブルDESによる暗号化処理を行なった構成例を示す。図29に示すように、各プロックのセクタ0は、鍵Kc

9にボリよフに、カノロックのたグラ 13. 強んで (0) とKC (1) の2つの線を用いてトリブルDES 毎号化を行ない、セクタ 5は、線KC (3) とKC (5 + 1) の2つの線を用いてトリブルDES毎号化を行な い、セクタM - 113. 線KC (M - 1) とKc (0) の 2つの線を用いてトリブルDES毎号化を行な立。 独合でも、ヘッグに格許する線数は、M国でもり、図2 7 (8) で示した總格辨数を超加させる必要はなく、セ

キュリティを高めることが可能となる。 【0181】さらに、図30に弱なる強様でのデータ暗

(2)

与化協成的を示す。図30は、メモリの各ブロックの2つの連続するセクタ領域を1つの暗号化プロックとして、2つの鍵を用いてトリブルDES暗号化を行なった。単様である。図30に示すように、各ブロックのセクタりとセクタ1は、鍵Kc(0)とKc(1)の2つの鍵を用いてトリブルDES暗号化を行ない、セクタ2sとセクタス+1は、鍵Kc(2s)とKc(2s+1)の2つの数を用いてトリブルDES暗号化を行ない、セクタM-1は、鍵Kc(M-2)とKc(M-1)の2つの数を用いてトリブルDES暗号化を行ない、セクタル-1は、鍵Kc(M-2)とKc(M-1)の2つの数を用いてトリブルDES暗号化を行ない、セクタル-1にが数C(M-1)の2つの数を用いてトリブルDES暗号化を行ない。となった。このように複数のセクタに同一の暗号化処理を適用することで暗号化プロセスを配りを表

(0182)図27,図29,図30に示す例の他にも、ヘッダに複数整格的し、その複数数から選択した。を現在機成としては環盤を用いて七クタ毎の暗号化を集行する構成としては環境が可能である。例えば、図27,29,30では、七クタ数と回数の鍵をヘッダに格納する構成としているが、例えば七クタ数がMのとき、格解整数をN(N</br>
人M)として、セクタのと七クタsは同じ鏡で暗号化する毎の構成としてもよい。また格辨整数をL(L>M)として、各七クタごとに全く異なる複数の鍵セットによる下リブルDESを適用する構成としてもよい。

3 ドンノルロンに出来り、3 1 (セクタ単位の改成チェック値(I C V )の付加係点)次に、セクタ単位の改成チェック値(I C V )の付加格成について説明する。視数セクタにまたがってが成在れるデータについて、その正当性を確認する場合、一般には、コンテンツデータ全体の最後などに削減した改成チェック値(I C V )を付加させる場成とするのが一般的であった。このようなデータ全体の同じ C V の付加制成においては、データを構成している各セクタ単位で、正当性を確認することができない。

(0184)また」CVを格的する場合、実データであるコンテンツの格的領域と同領領に「CVを入れ込むと、その分データ能として使用できる領域が減ってしまう。もし、各セクタにセクタ内のデータに対してセクタ毎の1CVを入れ込むと、デバイスのファイルシステムはデータが開催してデータを積み出す処理を共行するためのに、実際に使用されるデータを1CVから切り能して取り出すための処理。すなわちー度、第み出したデータ的のセクタ内の風、すなわちー度、第み出したデータ的のセクタ内の風、すなわちー度、第み出したデータがロークを複数となり、その処理を共行するためのファイルシステムを発入に、協策することが必要となり、その処理を共行するためのファイルシステムを発入に、協策することが必要となる。さらに、これらの1CVチェンクを傾動部で行うとなると、傾倒部にその処理の分の負荷がかかってしまう。

(0185)本税明のデータ処理装留においては、セクタ毎とデータ改成チェックを可能とするため、セクタ毎にデータ改成チェックを可能とするため、セクタ毎に「CVを設定し、その1CV設定位置を契データ領域ではなく、デバイスのファイルシステムによって認み取

られない函域として予め製成されている万長部領域とした。 冗長部に I C V を置く構成とすることで、データのに I C V を置く必要がなくなり、データ部の領域が多く利用できる。また、 冗長部に I C V を置くとで、データ部と I C V の切り分け・データ連結処理が不必要となるために、データ競み出しの連続性が保たれる。

(0186) データを辞み出す時には、メモリインタフェース部300(図2参照)でセクタ毎の1CVチェック処理を実行し、改度ありと判定され無効なデーダである場合は前倒部205(図2参照)への転送を実行しない。また、データ音音込み時には、メモリインタフェース部300において各セクタの1CVを計算して、冗長部に告きこむ処理を実行する。

[0187] なお、各セクタでICVを付加するかしないかを、セキュリティヘッダ(Security Header)に配置にて指定する。この構成については、図7のセキュリティヘッダ構成の説明中に示したように、セキュリティヘッダ中のICVフラグ(ICV Flag)が、プロック内のセクタ数(31セクタ)分のフラグを持ち、プロック内の各セクタのICV付加・非付加を示す。例えば0:1CVが2、1CVが30、として設定される。

(0188) 各セクタのデータ利用部と元長時構成を図31に示す。図31(3)のように、メモリ(フラッシュメモリ)に格納されるデータは複数のセクタ領域を持つプロック単位領域に分割して格納される。(b)に示すように、各セクタはデバイスのファイルシステムによって実データ(ex.コンデンツ)として部み取られる例えば512あるいは1024バイトのデータ利用部と、ファイルシステムによっては競み取られないECC(Brot Correction Code)等の情報を格約した元長部とによって相成される。

(0189) この元長部の容益は例えば16パイト、あるいは20パイトの予め決められた領域であり、デパイスのフィイルシステムは、この元長部を非データ領域として認識し、データ(コンデンツ)読み取り処理においては読み取らない。一般に、元長部に特辞的されるECCは、元長部全体を使用せず、元長部には非使用領域(リザーブ領域)が存在する。このリザーブ領域に各セクタの改竄チェック値(ICV)を格納する。

(0190) 元長郎にICVを格納した場合のデバイズのファイルシステムによるデータ部の連絡処理は、図31(c)に示すように、総粋にデータとして使用するものだけが格納されたデータ部の連絡を行なうのみの従来のデータ連絡処理と同様の処理が可能となる。従って、デバイスのファイルシステムは、元長部を除くデータ間破壊を単に連結すればよく、筋たな処理は何ら必要として破壊を単に連結すればよく、筋たな処理は何ら必要として

[0191] 本構成により、複数のセクタで構成されるデータのセクタ単位でデータの正当性の検証するにとが 田来る。また、故<u>値</u>チェック用のICVを冗長部に入れ

3

ることで、データ用に使えるデータ領域をそのまま活用 することが出来る。また、制御的には、1CVチェック の結果、正しい(改竄なし)と判定された正しいセクタ のみが送信される。また、1CVチェックがメモリイン タフェース部にて行われるので、制御部の負担がから ない等の効果がある。

[0192] [メディア内の国別数によるコンデンツ錠の保存処理]次に、メディア内の国別級によるコンデンツ盤の保存処理構成について説明する。先に、図7を用いて説明したように、コンデンツに対応して構成される七キュリディヘッダには、セクタ対応の暗号数としての複数のコンデンツキェック値生成数(Kicv\_Encrypted)が結号化されて格約されている。

[0193] これらの顔の暗中化の1つの蝴蝶は、予め デバイスのメモリインタフェースのメモリ語321 (図 4参照) に格辞されている配送館には、Fによって暗 年化して格辞さる構成がある。例えば、Kc\_Encryple 10=Enc (Kdist, Kc (0)) である。ここ で、Enc (a, b)は、bをaで暗号化したデータで あることを示す。このように、それぞれの鍵をデバイス の配送館には、5 はを用いて暗号化してたキュリティへ ッダに格許する構成が1つの構成である。

[0194] さらに、メディア2、すなわち時号処理部を持ち、デバイスとの相互認証を実行してコンテンツ処理を実行するメディアにおいて、メディア2の固有徴を用いてメディア2に結けするコンテンツに関するコンテンツキー、1CV生成盤を暗号化する顕体がある。以下、メディア2の固有鑑、ここではメディア2保存機Kstoを用いて信号化したコンテンツキー、コンデンツ1CV生成数をセキュリティヘッダに格料する処理について認明する。

(0195)メディア2保存鍵Kstotは、図2に示したようにメディア2、230のメディア2コントローラ231の内部メモリ235に格納されている。従って、メディア2保存盤Kstoや使用したコンテンツキー、1CV生成数の暗号化処理、省号処理はメディア2個で投行される。メディア2を装着したデバイスが、メディ投行される。メディア2を装着したデバイスが、メディをコンテンツ利用に扱いコンテンツが一の格料処理を実行するにもは、メディア2個で鍵の暗号化、従身処理を実行することが必要となる。本規明のデータ処理を実行することが必要となる。本規明のデータ処理を選信さいては、これらをCBのにCipher Block Chain ing) モードで処理することを可能とした。

(0196) 図32にCBCモードにおける数の暗句化処理構成を示す。この暗句化処理は、メディア2の暗句処理部236(図2参照)において実行される。内部メモリ236に格納された初期値1V\_ksysと、コンデンツチェック値生成鍵Kicv\_contとの排始論理和を実行し、その結果をメディア2の内部メモリ235に格納行し、その結果をメディア2の内部メモリ235に格納

された保存数K S t o を適用したD E S 暗号化を行ない、その結果をK i c v\_con1 Encryptedとしてヘッダ に格材する。さらに、K i c v\_con1 Encryptedとしてヘッダ に格材する。さらに、K i c v\_con1 Encryptedと、セ クタ (0) に対応するセクタが応コンデンツキーK c (0) との排他論理がを投行し、その結果をメディア3 の内部メモリ23 5に格材された保存数K S t o を適用 したD E S 信号化を行ない、その結果をK c (0) Encryptedと、さらに、K c (0) Encryptedと、セクタ (1) に対応するセクタが応コアンツキーK c (1) との排他論理がを投行し、その結果をK c (1) との排他機理がを投行し、その結果をK c (1) Encryptedとする。以下、これらの処理を維め返り 1 のを適用したD E S 信号化な行ない、その結果をK c (1) Encryptedとする。以下、これらの処理を維り返し、大力を指用に関います。以下、これらの処理を維り返し、大力を行して、ヘッダ格約用の総データとする。

ンテンシ改竄チェック値生成数 (Kicv) の生成が刊 メモリ235に格納された保存鍵Kstoを適用したロ ES復母処理を行ない、その結果を内部メモリ236ビ 格的された初期値 IV\_keysと排他論理和することによ Kc (0)が出力される。さらに、Kc (1) Encryple を行ない、その結果をコンテンツキーKc(0)Encryp る。以下、これらの処理を繰り返し抜行して、コンテン ツキーを取得する。なお、図には、コンデンツキーのみ を出力データとした例を示しているが、コンテンツ改竄 同様の処理が適用可能であり、暗号化されたコンデンツ 復号処理構成を示す。この彼号処理は、メディア2の略 り、セクタ (0) に対応するセクタ対応コンテンツキー ledと抜他論理和することにより、セクタ(1)に対応 チェック値生成数(Kicv\_Encrypled) についても [0197] 次に、図33にCBCモードにおける鮑の dに対して、保存鏈Kstoを適用したDES仮母処理 改竄チェック恒生成数(Kicv\_Encrypled)からコ 扩、K c (0)Bncrypledに対した、メディア2の内部 **するセクタ対応コンテンツキーKc(1)が出力され** 母処理部236(図2参照)において英行される。ま

能である。

(0198)上述のセクタ対応コンテンツキーKc(xx)またはコンチンツを設チェック値生成機(Klcv)の時時に、彼号処理に、多くの場合、メディア2を装むたデバイスからのコマンドに基づいて契行される。この場合、デバイスとメディアの同口は前述した相にしてコンテンツ両生、枯時等の様々な処理が残けされ、その一型のコンテンツの理型のロンとして上述のコンテンツキーの気号、命号に関係の関係が表してスとディア2回においてに認ってデンツキーの気号、命号にないでは、スカーKsesでは、相互移居時に生成したセッションキーKc(xx))をデバイスとメディア2回において促送する場合は、相互移居時に生成したセッションキーKsesで応号をされる。このセッションキーKsesで応号を出る。このセッションキーKsesで応号を出る。このセッションキーKsesで応号を出る。このセッションキーKsesで応号を出る。このセッションキーKsesで応号を出る。このセッションキーKsesで応号を出る。このセッションキーとのによる信号

キュリティを高めることが可能となる。

ナタ。デバイス倒では、受信したデータ列K c (0) En crypled~K c (M-1) Encrypledについて、メディア **2 との相互認証時に生成したセッションキーKsesを** 適用して、図33と同様のDES-CBCモードでの復 **母処理を実行することによりコンテンツキーK(c)を** のみを処理データとした例を示しているが、コンテンツ **適用したDES-CBCモードでの暗号化処理を実行す** Encrypted~K c (M-1) Encryptedをデバイスに送価 [0200] これらの出力された結果をさらに、デバイ スとの相互認証時に生成したセッションキーKSeSを 取得することができる。なお、図には、コンテンツキー 改成チェック値生成数(Kicv\_Encrypled)につい **る。その結果得られたSE0~SEM-1:Kc(0)** ても同様に処理データとして構成することが可能であ 出力結果としてのコンテンツキーを取得する。

号化塩様は、上述したようにセクタ毎に異なる麴で暗号 化した態様と、コンテンツ全体を1つの暗号化数で暗号 化した塩様とがあり、これらは、ヘッダの情報に基づい の制御部、右側はデバイスのメモリインタフェースの処 [0201] [暗号化データの既み出し処理] 図35以 下のフローを用いて、暗号化されたデータのメディアか らの試み出し処理の詳細を説明する。なお、データの暗 て判定される。図35のフローにおいて左側はデバイス

[0202] まず何御部は、蜆み出し対象となるコンテ ンツのヘッダファイルを睨み出す (S701)。 この処 理は、前述の図25のファイル既み出し処理フローに従 った処理として実行される。次にヘッダセットコマンド と、読み出したヘッダファイルをメモリインタフェース に送信 (S702) する。

チェックは、先に図14を用いて説明したICV生成処 理において、セキュリティヘッダ検証値生成變Kicv タを入力して11 CV、を生成し、生成した1 CV、と予 **めヘッダに格納された 1 C V とを照合する処理によって** [0203] メモリインタフェースはヘッダセットコマ ンドを受信 (S 7 0 3) すると、ビジーフラグを 1 (ビ ジー) にセット (S104) し、ヘッダの改設チェック 値(1 CV)を検証(S 7 0 5)する。ヘッダの1 C V \_\_s nと、初期値 1 V s hを適用してヘッダの構成デー

5。例えば、自デバイスで生成し格納したコンテンツを メモリに格納するとき毎は、リポケーションリスト・バ [0204] 検証によりヘッダ改竄なしと判定 (S70 - ションを0として、再生処理等の際にリポケーション 6) されると、ヘッダ内の有効リポケーションリスト・ パーションが0でないかがチェック(S707)され リストを非参照とした処理を実行可能とする。

場合は、リポケーションリストを参照する必要がないの する処理として、ステップS113でヘッダセット成功 [0205] リギケーションリスト・バーションが0の でステップS710に進む。パージョンが非0であると ヘッダのバージョンより古くないかをチェック(S 7 0 8)し、古い場合は、3~13に猫み、ヘッダセット成 カフラグを0(NG)に設定して処理を終了する。セッ トされているリポケーションリストがヘッダのバージョ ンより古くなければ、ステップS109に進み、リポケ - ションリストを参照して、読み出し対象のコンデンツ Dがないかを判定する。あった場合は読み出しを禁止 きは、現在セットされているリポケーションリストが、 フラグを0 (NG) として処理を終了する。

ーKcと、コンテンツチェック値生成盤Kicv\_conf 後は、メデイアの装着時、コンテンツの再生時において メモリインタフェースにおいて総統的に利用可能とした テンツ1 Dが記録されていなければ、ステップ5710 **進み、ヘッダ情報に基づいて暗号化されたコンテンツキ** 6の起動時フローにおいて説明したように、起動時にメ モリインタフェースにセットアップされ、セットアップ 【0206】 リポケーションリストに記み出し対終ロン を復号する。なお、リポケーションリストは、先の図1 リポケーションリストである。

ュリティヘッダの中には、前述のセクタ毎に適用する時 (M-1)が暗号化されて格納されている。また、コン テンツの改竄チェック値 (ICV)を生成するためのコ ソアンシアコック値生成盤Kicv\_confも暗号化され 【0207】先に、図7他を用いて説明したようにセキ **<b><b>小窓かしたの放牧のロソ**アソシキーK c (0) ~K c て格納されている。

た、コンドンシキーK c (0) ~K c (M−1) を徴号 [0208] コンテンツの復号に先立ち、これらのコン アンツチェック値生成鍵Kicv\_contを復号してコン テンツの改竄チェックを実行する処理が必要であり、 **「る処理が必要となる。** 

る。図37の処理は、デバイスのメモリインタフェース における処理である。図4の暗号処理部320において c、コンナンシチェック値生成観Kicv\_\_con1の復号 処理フローを示す。囚31の各ステップについて説明す (0209) 図37に届与化されたコンテンツキーK

[0210] まず、暗号化コンテンツチェック値生成処 Kicv\_conlを復号対象として遊磨(S 8 0 1)し、

場合は、前述の図27他で説明したセクタ単位の暗号化 ーマットが0である場合は、コンテンツ全体をセクタに 母化フォーマットタイプ・フィールドの設定が 1である 塾を用いた方法である。セクタ単位の暗号化塾を用いた 方法である場合は、ステップS803に進み、セクタ毎 **火に、ヘッダの暗号化フォーマットタイプ・フィールド** の設定が0か否かを判定(S802)する。暗号化フォ **除わらず 1 つの暗号化塩様としたデータ構成であり、略** に設定された暗号化コンテンツキー(K c\_Bncrypled0 ~31) を復号対象にする。

0であると判定された場合は、ステップ3804できら して1 (トリブルロES)が0 (シングルロES) であ るかを判定する。シングルDESである場合は、ステッ 【0211】ステップS802で暗号化フォーマットが に、ヘッダの暗号化アルゴリズムフィールドをチェック **がS805で1つの粨串代コンアンシキー(Kc\_Encry** ある場合は、ステップS806で複数の暗号化コンテン pled0)のみを復号対象として加え、トリブルロESで ツキー(K c\_EncrypledO, 1)を彼号対象として加え

のコンテンツタイプフィールドの設定をチェックし、歌 定が2 または3 (メディア2の格納コンテンツ) でない 場合は、ステップS808で、メモリ部321(図4秒 すなわち、暗号化コンテンツチェック値生成**差**Kicv [0212] 次に、ステップS807において、ヘッダ 照)に格納された配送機K d i s t で復号対象データ、 \_con1と、1以上のコンテンツキーを復号する。

テンツ)である場合は、ステップS809で彼号対象デ ータ、すなわち、暗号化コンテンツチェッグ値生成機K の保存難Ksto(CBCモード)で復号する。この復 号処理の詳細は、図32、図33、図34を用いて説明 [0213] 設定が2または3(メディア2の格納コン i c v \_con1と、1以上のコンテンツキーをメディア2 した通りである。

\_con1と、1以上のコンテンツキーKcの復号処理につ ディア 2のコントローラ (図2参照)の処理を示してい [0214] ステップS809におけるメディア2の保 存盤による暗号化コンテンツチェック値生成盤Kicv いて図38のフローを用いて説明する。図38のフロー は、左側にデバイスのメモリインタフェース、右側にメ

スは、各鍵を順次送信(S 1004)し、メディア 2コ ントローラが仮与対象データK(i)を受値(S 1 0 0 ゲータK (0) ~K (n-1) (語号化コンテンツチェ [0215] まず、メモリインタフェースは、仮号対象 ッケ価缶段盤Kic v \_con(A、1以上のコンドソシキ 一) を設定 (S1001) L, CBC包号初期化コマン メディア 2コントローラは 1 V K e y s をレジスタにセ ット (S1005) する。 その後、 メモリインタフェー ドをメディア 2コントローラに送信(S1003)し、

**업母対象データK(i)に対して、メディア2の保存数** る。次に、メディア2コントローラは、仮号粒データ列 (S1007) し、彼母された鰡データ (ex. 複数の によってCBCモードでの暗号化処理を実行し、データ [0216] 次にメディア2コントローラは、受信した を、デバイスとの相互認証時に生成したセッションキー Kstoを用いたCBCモードによる紅号処型を英行 セクタ対応コンテンツキー)を取得 (S1008) す

列K'(i)を生成して、結果をデバイスに送信(S1 009) する。ステップS1007~S1009の処理 は、先に説明した図34のDES-CBCモードによる

K' (i) を受信し、すべてのデータを受信したことを 確認の後、CBC終了コマンドをメディア 3コントロー マンドの受傷によりレジスタをクリア(S 1 0 1 4)す ラに送信する。メディア 2コントローラはCBC終了コ 【0217】 デバイスのメモリインタフェースは、 慰次 処理に基づいて実行される。

用い、メディア2との相互認証時に生成したセッション キーKsesを適用してCBCモードでメディア 2から [0218] デバイスのメモリインタフェースは、メモ S1015)する。この彼号処理は、先に説明した図3 り部321 (図4参照) に格納した初期値1V\_keysを 受信したK' (i) を包号 (S1010~S1013, 3の構成と回様の処理である。

[0219] 上記処理により、デバイスは、ヘッダに格 材された暗号化されたコンテンツキーK c、コンデンツ チェック値生成盤Kicv\_conlを仮号し、それぞれの 処を取得することができる。 [0220]次に図35に戻り、暗号化ファイルの航み 出し処理の枕きを説明する。上記の勉徴号処理ステップ であるステップS110を修了すると、ステップS11 ンタフェースはヘッダを「銃み出しヘッダ」として内部 に設定し、ヘッダセット成功フラグを1 (成功) にセッ る。コンテンツ競み出しに扱しては、設定されたヘッダ 1に進む。ステップS711では、デバイスのメモリイ トし、ビジーフラグを0 (特(g) (S714) 散定す

データス競み出しコマンドをメモリインタフェースに送 [0221] 一方、傾仰部側は、ステップS715でス ヘッダセット成功フラグが1 (成功) (S717) とな 信し、ビジーフラグが0(特徴)(S716)であり、 ったことを条件として次の処理(図36)に進む。 の情報に基づく処理が実行される。

[0222] 図36のステップS721において、傾倒 智は、ファイル包の当てアーブルから読み出し対象のコ ンデンツファイルのセクタアドレス (S (1) ~S

[0223] メモリインタフェースは、セクタS (i) (K) ) を取得し、メモリインタフェースに対して即 次、セクタS(i)競み出しコマンドを送信する。

68

は、受信セクタS(i)が内部メモリか、外部メモリで ィアが有効にセットされていることを示す)であるかを 丁)を参限して、BPTが読み出し対象であるセクタS かを判定 (S729) する。BPTに飲み出し許可プロ 【0224】ヘッダ成功フラグが1(成功)である場合 は、メディア1かメディア2のセットフラグが1(メデ (i) を読み出し許可対象プロックとして設定している ックの設定がある場合には、外部メモリから鼓当セクタ あるかを判定 (S727)し、外部メモリである場合 判定 (S728) し、セットフラグが1である場合に は、さらにプロックバーミッション・テーブル (BP のデータを読み出す (S730)。

が1でない場合、または、BPTにセクタS(i)の乾 み出し許可が設定されていない場合には、ステップS7 管理のなされていない内部メモリ内のデータである場合 わちセクタS(i)を格納したメディアのセットフラグ 38に進み、航み出しエラーとして航み出し成功フラグ ップS728、S729の判定がNoである場合、すな [0225] なお、読み出し対象データがBPTによる は、ステップS128,S729はスキップする。ステ がりにセットされる。

[0226] ステップS726~S729の判定プロッ クにおいて、対象セクタS (1) の飢み出しが実行可と 判定されると、メモリから被当セクタが銃み出され、セ クタに対応して設定されている冗長部の関り訂正符号に 払づく限りII正処理が実行 (S731)され、限りII正 クタが改成チェック値 (ICV) による処理対象である かを判定する。先に図3~で用いて説明したように各セ クタは、その冗長部に改竄チェック用の1 CVを格納し が成功した(S132)ことを確認する。次に、ヘッダ の1CVフラグ (図7参照)を参照し、読み出し対象セ ており、セクタ単位での改竄チェックが可能である。

合は、ステップS734において、ステップS710の ク対象データ(セクタデータ)を入力して図14を用い [0227] ICVによる改竄チェックの対象である場 **復号処理によって得たコンテンツチェック値生成数Ki** c v\_contと、初期値1Vcontを適用し改竄チェッ セクタの冗長部に格納されている1CVとの照合を行な て説明した100生成処理を実行し、100 を求め い一致していれば改成なしと判定する。

ると、ステップS737に進み、ヘッダ情報に基づいて {0228] ICVチェックにより改竄なし七判定され (成功) に設定し、復号データをパッファに格納する。 データの彼号処理を実行して眺み出し成功フラグを1

46において、メモリインタフェースのステーケスを耽 をパッファから取り出して保存し、アドレスを鬩次イン 保存する処理を繰り返し実行し、すべての既み出し対象 み出して、ピジーフラグが0の状態において、競み出し 丸功フラグが 1 であることを条件として説み出しデータ **クリメントして、データを顧次パッファから取り出して** ヒクタを保存した後、全説み出しセクタデータからファ 10229] また、癒御部は、ステップS740~S7 イルを構成して処理を終了する。

処理の詳細を図39を用いて説明する。この彼号処理は [0230] 図36のステップS736のデータ部値号 デバイスのメモリインタフェースの暗号処理部320

1101)。 次にそのセクタが暗号化対象であるかをチ エック (S1102) する。このチェックは、セキュリ [0231] まず、彼号対象のデータ格納セクタ位置を s (0≦s≦31 (セクタ数32の場合)) とする (S ディヘッダ(図7参照)の暗号化フラグ(Bucryption F (図4参照)において実行される。

号化フォーマットタイプ (Encryplion Formal Type) の (S1103) する。これはセキュリティヘッダ内の暗 設定をチェックするものであり、図8で説明したコンテ ンツ全体を1つの暗号化態隊としているか、各セクタに 異なる鍵を用いた暗号化処理を行なっているかを判定す は、彼母処理は実行されず、処理は終了する。暗号化対 **象である場合は、暗号化フォーマットタイプをチェック** lag) に基づいて判定される。暗号化対象でない場合

【0232】 暗号化フォーマットタイプ (Encryption P ステップS1104において、暗号化アルゴリズム (En cryption Algorithm)の判定を行なう。暗号化ブルゴリ ormal Type) の設定値が0の場合は、コンテンツ全体を **煎)かを設定しているものであり、シングルロESであ** 1つの商号化態様としている場合である。この場合は、 ズムは、シングルロESかトリブルロES (図28巻 ると判定された協合は、1つのコンテンツキーK c

(S1106) する。トリプルロESであると判定され (0) を適用して暗号化コンテンツの復号処理を実行 (1)を適用して暗号化コンテンツの復号処理を実行 た協合は、2 つのコンデンシキーK c (0)、K c

5 において、暗号化アルゴリズム (Encryption Algorit 111) の判定を行なう。 暗号化アルゴリズムは、シングル **{0233} 一方、ステップS1103で、暗舟フォー** の場合は、各セクタに異なる塾を用いた暗号化処理を行 なっている場合である。この場合は、ステップS110 マットタイプ (Encryption PormaiType) の設定値が1 (\$1107) \$5.

DESかトリブルDES (図28参照) かを設定してい るものであり、シングルDESであると判定された場合 ーKc(s)を各セクタに適用して略卑化コンデンシの

は、各セクタ(s)に対応して設定されたコンテンツキ

**뒻号処理を実行 (S1108) する。トリブルDESで** (s)、Kc(s+1mod3 2)を適用して合セクタ 毎の暗号化コンテンツの復号処理を実行(S 1 1 0 9) あると判定された場合は、2つのコンテンツキーKc

108と同様である。ステップS1209~S1211 【0234】セクタデータの彼号処理の異なる処理館様 ~51208は、図39の各ステップ51101~51 を図40に示す。図40において、ステップS120

[0235] ステップS1205において、暗母化アル ゴリズムがトリブルDESであると判定された場合、ス テップS1209においてセクタNo. (s)を判定 し、sが奇数である場合は、s=s-1の更新を実行 (S1210) し、各セクタに適用する鍵をK c が図39とは異なる。

号処理を伴う再生処理は、図35~図40を用いて説明 (s), Kc (s+1) としてトリブルDESによる数 [0236]以上、暗号化されて格納されたデータの役 母処理 (S1211) を実行する。

[0237] [データの暗号化音き込み処理] 次に、図 41以下のフローを用いて、メディアに対するデータの 化塾で暗号化した鼠様とがある。これらは、ヘッダ情報 に散定される。図41のフローにおいて左側はデバイス の制御部、右側はデバイスのメモリインタフェースの処 データの暗号化態様は、上述したようにセクタ毎に異な る勉で暗号化した協様と、コンテンツ全体を1つの暗号 暗母化審き込み処理プロセスの詳細を説明する。なお、 したようなプロセスにより実行される。

[0238] 虫ず制御部は、競み出し対象となる格納コ ンデンツに対応するヘッダ生成コマンドとヘッダ惰頼と してのパラメータをメモリインタフェースに送信する。 (\$1301).

を0に設定 (S1305) し、リポケーションリストの り、リポケーションリストの非砂瓶でのデータ処理(再 10においてヘッダ生成成功フラグを0 (NG) に設定 [0239] メモリインタフェースはヘッダ生成コマン ドを受信 (S1302) すると、ピジーフラグを1 (ピ ジー) にセット (S1303) し、受信パラメータが貯 容値内であるかを判定(S 1304)する。メモリイン **タフェースは、予めヘッダに設定可能なバラメータ範囲** を有しており、受信パラメータと比較し、受信パラメー タが設定可能範囲を超えている場合は、ステップS13 して処理を終了する。受信パラメータが許容値内である 場合は、ヘッダの有効リポケーションリストバージョン 非参照でのデータ処理を可能とする。有効リポケーショ ンリストパージョンを0として設定するのは、自デパイ スでの格納処理を行なったコンテンツについては正当な コンデンツであることが保証されているとの前提によ

段を介して外部から受信したコンテンツであり、受信コ のリポケーションリストとの限合が可能であれば、上記 処理の代わりに、先に図35を用いて説明したファイル **復号銃み出し処理において実行されるステップS707** ~S709と同様のリポケーションリストを用いた職別 ンテンツに類別子が付加され参照すべきリポケーション リストパージョンをヘッダに格納しておりデバイス内部 [0240] なお、雷き込みコンテンツが例えば返信手 子照合処理を行なってもよい。

が情報に払びいトロンテンシキーKo、ロンドンシ政院 [0241] 次に、ステップS1306において、ヘッ チェック値(ICV)生成盤Kicv\_conlを生成、時 は、デバイスのメモリインタフェースの略号処理部32 0 (図4 参照) において実行される。図43のフローに **母化する。ステップS1306のコンテンツキーKc、** コンテンジ设置チェック値生成盤Kicv\_confを生 成、暗号化処理の詳細を図43に示す。図43の処理 ついて説明する。

化対象とし(S1401)、次に、ヘッダの暗号化フォ Kicv\_conlを、例えば乱数に払づいて生成し、暗号 【0242】まず、昨号化コンテンツチェック恒生成勉 **ーマットタイプ・フィールドの設定が 0 か否かを判定** 

(S1402) する。 暗号化フォーマットが0である切 **夕単位の暗号化鍵を用いる場合は、ステップS1403** (0) -Kc (31) (セクタ数32の協合)) を生成し 合は、コンテンツ全体をセクタに係わらず.1つの暗号化 路様とする梢成であり、暗号化フォーマットタイプ・フ メールドの設定が1である場合は、前近の図27位で説 明したセクタ単位の暗号化繳を用いる方法である。セク に進み、セクタ毎に設定されたコンテンツキー (K c

が0であると判定された場合は、ステップS1404で さらに、ヘッダの暗号化アルゴリズムフィールドをチェ [0243] ステップS1404で邸母化フォーマット ックして1(トリブルロES)か0(シングルDES) であるかを判定する。シングルDESである場合は、 **で暗号化対象とする。** 

(0)) を生成して暗号化対象として加え、トリブルロ ESである場合は、ステップS1406で位数のコンテ **ソシキー(K c (0)、K c (1))を生成した柜与化** テップS1405で1つのコンテンツキー (Kc 14余として加える。

い場合は、ステップS1408で、メモリ部321(図 [0244] 次仁, ステップS1407において, ヘッ 4 参照)に格材された配送数Kdistでデータ、かな 設定が2または3(メディア2の格納コンテンツ)でな ゲのコンテンツタイプフィールドの設定をデェックし、 むも、コンドンシヂェック値虫成骸Kicv\_coulと、 1以上のコンテンツキーを暗号化する。

[0245] 設定が2または3(メディア2の格納コン テンツ)である協合は、スチップS1409でデータ、

生)を可能とする設定を行なうものである。

ディア2のコントローラ(図2参照)の処理を示してい [024.6] ステップS1409におけるメディア2の 保存塾によるコンテンツチェック値生成拠Kicv\_co nlと、1以上のコンテンツキーKcの略号化処理につい は、左側にデバイスのメモリインタフェース、右側にメ て図44のフローを用いて説明する。図44のフロー

る。次に、メモリインタフェースは、CBC暗号化初期 化コマンドをメディア 2コントローラに送信する。メデ イア2は、メディア2の内部に格納している初期値1V \_keysをレジスタにセット (S1506) する。そ CBCモードによる暗号化対象データK (0) ~K (n - 1) の届电行や政行し、アータK' (0) ~K' (n 先に説明した図32と同様の処理構成において実行され の後、メモリインタフェースは、各麭を鬩次送信(S I テンツキー) を設定 (S1501) し、メディア 3との 相互認証時に生成したセッションキーを適用し、メモリ [0247] まず、デバイス回のメモリインタフェース in、 品电行対後データK(0)→K(n−1)(コンデ ンシチェック値生成数Kicv\_contと、1以上のコン 部321に格納した初期値IV\_keysを用いてDES-- 1)を生成 (S1502) する。この暗号化処理は、 505) \$5.

による暗号化処理を実行し、データ列K"(1)を生成 して、格果をデパイスに送信 (S1510) する。ステ 34のDES-CBCモードによる処理に払づいて実行 ップS1501~S1510の処理は、先に説明した図 (1) に対して、デバイスとの相互認証時に生成したセ ッションキーによって CB Cモードでの復号処理を実行 (S1508) し、彼号された鮑データ (e x. 複数の る。次に、メディア2コントローラは、彼号塾データ列 を、メディア 2の保存機K s t oを用いたCBCモード セクタ対応コンテンツキー)を取得 (S1509) す [0248] メディア 3コンドローラは、データK' (i) を受信 (S1501) し、受信したデータK'

K" (i) を受信し、すべてのデータを受信したことを ラに送信 (S1511~S1514) する。メディア 2 コントローラはCBC終了コマンドの受信によりレジス 【0249】デバイスのメモリインタフェースは、鬩次 **偏認の後、CBC椅了コマンドをメディア2コントロー** 

ィア2から受信したK" (0) ~K" (n~1) をヘッ ダ格納用の暗号化麭データとする。 上記処理により、デ 【0250】デバイスのメモリインタフェースは、メデ タをクリア (S1515) する。

−Kc、コンテンツチェック値生成盤Kicv\_contを パイスは、ヘッダに格納する暗号化されたコンテンツキ

エック値ICVを生成(S1307)する。セキュリテ インタフェースは生成したヘッダデータに基づく改竄チ イヘッダのチェック値であるICV\_shは、メモリ部 を用いて、先に図14を用いて説明した1CV生成構成 (成功) としてビジーフラグを 0 (特機) として処理を [0251] 図41に戻り、ファイルの暗号化書き込み 処理の説明を続ける。ステップS1306において、上 述のヘッダ格納鍵の生成、暗号化が終了すると、メモリ 321 (図4╋限) に格納された初期値 IVshと、セ キュリテイヘッダ改竄チェック値生成轍Kicy\_sh に基づいて生成される。次に、ステップSI308で、 生成されたヘッダを留き込みヘッダとして内部に保存 し、ステップS1309でヘッダ生成成功フラグを1

となったことを条件として、バッファからヘッダを競み ステータス銃み出しコマンドをメモリインタフェースに 送信し、ピジーフラグが0(待機)(S1313)であ 田し、選絲のファイルとしたメディアに保存(S131 [0252] 一方、桐御部側は、ステップS1312で り、ヘッダ生成成功フラグが1 (成功) (S1314) 5)後、次の処理(図42)に進む。

[0253] 図42のステップS1321において、制 S (i) を設定して、メモリインタフェースにセクタ S (i) の暗号化智き込みコマンドと、データD (i) を **頤次送信(S1321~S1324)する。 メモリイン** タフェースは、セクタS (i) 暗号化魯き込みコマンド を受信 (S1325) すると、ピジーフラグを1 (ビジ ー) に設定(S1326)し、ヘッダ生成成功プラグが 1 (成功) である (S1327) ことを条件として次ス る。制御部は、次に各データロ(i)の告ぎ込みセクタ 御部は、碧き込み対象のコンテンツファイルをセクタに 分割する。分割されたデータを口(1)~口(k)とす アップに進む。

がある場合には、セクタに対応して設定する限り訂正符 セットされていることを示す)であるかを判定(S13 て、BPTが碧き込み対象である七クタS(i)を告き 込み許可対象プロックとして設定しているかを判定 (S 1330) する。日PTに雪き込み許可プロックの設定 【0254】次に、メモリインタフェースは、受信セク タS(i)が内部メモリか、外部メモリであるかを判定 (S1328) し、外部メモリである場合は、メディア 1 かメディア 2のセットフラグが 1 (メディアが有効に 29) し、セットフラグが1である場合には、さらにプ ロックパーミッション・テーブル (BPT) を参照し 号を生成 (S1331) する。

クタであるか否かをヘッダ情報 (ICVフラグ) に基づ [0255] 次に、その魯き込みセクタが1CV設定セ

コンテンシ I C V 生成器K i c v \_confic 払びらたもク いて判定 (S1332) し、1 CV 対象である場合は、 タデータに対する1CVを生成 (S1333) する。

5を用いて説明する。この暗号化処理はデバイスのメモ リインタフェースの暗号処理部320(図4参照)にお [0256] 次に、メモリインタフェースは、ヘッダ僧 ステップS1334のデータ部時号化処理の詳細を図4 粗に基づくデータの暗号化を実行(S1334)する。

いて実行される。

ック (S1603) する。これはセキュリティヘッダ内 [0257] まず、暗号化対象のデータ格納セクタ位置 をチェック (S1602) する。このチェックは、セキ 合は、暗号化処理は実行されず、処理は終了する。暗号 の暗号化フォーマットタイプ (Encryption Pormal Typ コンテンツ全体を1つの暗号化塩様としているか、各セ クタに異なる鮑を用いた暗号化処理を行なっているかを (S1601)。 次にそのセクタが暗号化対象であるか ュリティヘッダ (図7 参照) の暗号化フラグ (Bncrypli 化対象である場合は、暗号化フォーマットタイプをチェ Ou Flag) に基づいて判定される。略与化対象でない場 e) の設定をチェックするものであり、図8で説明した を s (0≦ s ≤ 3 1 (セクタ数 3 2 の場合)) とする

[0258] 暗号化フォーマットタイプ (Encryption F (0)を適用して時号化コンテンツの暗号化処理を実行 ステップS1604において、暗号化アルゴリズム (En **限)かを設定しているものであり、シングルロESであ** ormal Type) の設定値が0の場合は、コンテンツ全体を cryption Algorithm)の判定を行なう。暗号化アルゴリ 1つの時号化類様としている場合である。この場合は、 ズムは、シングルDESかトリブルDES (図28巻 ると判定された場合は、1つのコンテンツキーKc

(S1606) する。トリプルDESであると判定され (1)を適用して暗号化コンテンツの暗号化処理を裏行 **た協会は、2 ンのコンテンシキーKc(0)、Kc** 

(S1607) \$5.

かトリプルDES (図28参照) かを設定しているもの (5) を各セクタに適用して暗号化コンテンツの暗号化 処理を実行(S1608)する。トリブルDESである [0259] 一方, ステップS1603で, 暗号フォー の場合は、各セクタに異なる鍵を用いた暗号化処理を行 なう場合である。この場合は、ステップS1605にお いて、商号化アルゴリズム (Encryption Algorithm) の 判定を行なう。暗号化アルゴリズムは、シングルDES であり、シングルロESであると判定された場合は、各 セクタ(s)に対応して設定されたロンデンツキーK c (s)、Kc (s+1mod32)を適用して各セクタ マットタイプ (Encryplion FormalType) の設定値が1 と判定された場合は、2つのコンデンツキーKc

を図46に示す。図46において、ステップS1701 [0260] セクタデータの復号処理の異なる処理態様 -S1708は、図45の各ステップS1601~S1 608と同様である。ステップS1709~S1711

ゴリズムがトリブルDESであると判定された場合、ス [0261] ステップS1705に枯いて、暗母化アル テップS1709においてセクタNo. (s) を判定 し、sが奇数である場合は、s=s-1の更新を実行 (S1710)し、各セクタに適用する観をKc

(s), Kc (s+1) としてトリブルDESによる徴 処理フローの説明を続ける。上述の処型によってデータ [0262] 図42に戻り、ファイルの昨号化省き込み 号処理 (SI711)を実行する。

部をメディアに雪を込み(S 1336)、智を込み成功 し、暗号化されたデータロ(i)とセクタデータに対応 する改麿チェック値1 C V と、殴り们正符号を持つ冗長 フラグを1 (成功) にセット (S1337) し、ビジー 郎の暗号化処理ステップ (S1334) が徐了小ると、 データ部に対する限り町正布号を生成 (S1335)

フラグを0 (特徴) に設定 (S1339) する。

可が設定されていない場合には、ステップS1338に [0263] なお、哲食込み対象データがBPTによる 管理のなされていない内部メモリ内への替き込み処理で ある場合は、ステップS1329,S1330はスキッ ブする。ステップS1329、S1330の判定がNo である場合、すなわちメディアのセットフラグが1でな い場合、または、BPTにセクタS(1)の皆き込み許 個み、母を込みエラーとして告き込み成功フラグを0に セットする。

346)し、更新したファイル勧り当てテーブルを更新 コマンドとともにメモリインタフェースに送信(S 1 3 [0264] また、飼御部は、ステップS1341~S 1345において、メモリインタフェースのステータス を銃み出して、ピジーフラグが0の状態において、皆き 込み成功フラグが1であることを条件としてアドレスを 間次インクリメントして、毎き込みデータを脳次メモリ 47)し、メモリインタフェースはコマンドに従ってフ アイル割り当てテーブルの哲を込み処理を実行 (S13 インタフェースに送信する。すべての処理が終了する と、ファイル割り当てテーブルの更新処理を実行(S

[0265] 以上の、図41~図46によって説明した 処理により、データの暗号化、メディアに対する格納処 理が英行される。 40) \$5.

**うに、本発明におけるリポケーションリストは、複数の** ションリストの更新処理について説明する。前述したよ 【0266】 [リポケーションリストの延断] 次に、不 正なメディアやコンテンツの失効徴報としてのりポケー **啞盤(ex、メディア、コンテンツ)の殻別子(1D)** 

8

モリ・インターフェース部において、利用メディアまた **京型用コンナンシの韓別子(1D)と、リボケーション** リストのリスティング1Dとの照合を実行することによ り、不正なメディアの使用や不正なコンテンツの読み出 から協成される。コンテンツやメディアの失効情報であ の孤類のコンテンツ、メディアを排除することが可能と なる。メディアの抑入時やコンテンツの乾み出し時にメ 行うことによって、1 つのりポケーションリストで複数 るリポケーションリスト (Revocation List) に複数の 価類の10を設け,それぞれの照合を異なる動作として しを禁止することができる。

トには、リボケーションリストバージョン (Revocation [0267] 先に説明したように、リポケーションリス コンデンツの失効惰粗を追加した場合等にリポケーショ List Yersion) が設定され、新たな不正なメディアや ンリストは更新される。

【0268】リポケーションリストの更新処理フローを 図47に示す。図47において、左側はデバイスの制御 【0269】まず、制御部は更新用のリポケーションリ ストを通信部201 (図2参照) から受信する (S18 01) と、更新用りポケーションリストチェックコマン ドと、受償した更新用りポケーションリストをメモリイ 14、右側はデバイスのメモリインタフェースである。 ンタフェースに送信 (S1802) する。

ーフラグを1 (ピジー) に設定 (S1804) し、リポ ケーションリストの改竄チェック値(1CV)生成鏈K 【0270】メモリインタフェースは、更新用リポケー ションリストチェックコマンドと、更新用リポケーショ ンリストを制御部から受信 (S1803) すると、ビジ i c v\_r 1を生成 (S 1805) する。

[0271] リポケーションリストの改成チェック用の cv\_rlと、リポケーションリスト (Revocation List) の ーションリストの属性情報中に含まれるリポケーション めデバイス内に格納されたリポケーションリスト (Revo 1 CV鍵を生成する時の初期値:1 Vicv\_rlと、リポケ 具体的には、改竄チェック値(1CV)生成麭Kicv 類値(ⅠVicv\_ri)の排色簡單和にマスター館:MKic ハ\_イ」によるDESモードでの暗号化処理を実行するとい calion List)の1 C V飽を生成するマスター麭:MKi 改竄チェック値(1 C V)生成姫Ki c v\_r l は、予 1) に払づいて改成チェック値(1 C V)生成轍が生成 される。前記式の意味は、バージョン (Version) と初 \_r ! = DES (E, MKicv\_rl, Yersion I Vicv\_r リスト・バーション(Version)に格づいて生成する。 う類味である。

【0272】次にメモリインタフェースは生成した改竄 予めリポケーションリスト内に格納された正しい 1 C V値と照合1 C V′=1 C V Pを実行 (S 1807) チェック値(1CV)生成粒Kicv\_rlを用いてリ ポケーションリストの1CV'を生成(S1806)

する。なお、ICV,の生成処理は、前述の図14で説 明したDESモードに基づいて、初期値1Vclを用い、 虫成した改竄チェック値(1 C V)生成額Ki c v\_r |を適用した処理によって行われる。

ョンリストのパージョンが新しい場合には、更新用リポ 0) し、ビジーフラグを0にセット (S1811) して い正当なものであると判定され、ステップS1808に **過み、現在セットされているリポケーションリストのパ** ージョン (i) と更新用リポケーションリストのパージ (0273) 1CV = 1CVである場合 (S1807 でYes)は、更新用りポケーションリストが改成のな ョン (i) を比較 (S1809) し、更新用リポケーツ ケーションリストの有効フラグを1に設定(S181 処理を終了する。

し、ビジーフラグが0となった (S1813) ことを頒 恩し、更新用りポケーションリスト有効フラグが1 (S 1814) である場合に、更新用リポケーションリスト 【0274】一方、制御部側は、ステータス競み出しコ を通常のファイルとして内部メモリに保存 (5181 マンドをメモリインタフェースに送信(S 1812)

5) する。コンテンツの処理、メディアの装着時のチェ ックの際には、内部メモリに格納されたリポケーション リストが読み出される。

明について群解してきた。しかしながら、本発明の要旨 (0275)以上、特定の実施例を参照しながら、本発 を逸脱しない範囲で当業者が該英施例の修正や代用を成 し得ることは自明である。すなわち、例示という形態で 本発明を開示してきたのであり、限定的に解釈されるペ きではない。本発明の要旨を判断するためには、冒頭に 記載した特許請求の範囲の福を参酌すべきである。

て、BPTにおいて許可された処理である場合にのみ記 **徴手段に対するアクセスを実行し、BPTに遠反する処** するアクセスが実行されるので、例えば留き換えを禁止 している記録メディア内のデータ(コンテンツ)の勧告 臭えを効果的に防止し、コンテンツの保護を高めること ンタフェースに設定したテーブルに従って記憶手段に対 許可情報に基づいたアクセス許可テーブルであるブロッ [発明の効果] 以上、説明したように、本発明のデータ 処理装置、データ配憶装置、およびデータ処理方法によ れば、例えばフラッシュメモリを搭載したメモリカード **毎のデータ記憶手段に対するアクセスにおいて、デバイ** スのメモリインタフェース部に予め定められたアクセス 理要求に対しては処理を行なわない構成としたので、劇 **卸部の処理内容、コマンドにかかわらす、常にメモリイ** ク・パーミッション・テーブル (BPT) をセットし (0276)

[0277]また、本発明のデータ処理装置、データ記 食装置、およびデータ処理方法によれば、プロック・パ **ーミッション・デーブル(BPT)を格約した領域は、** 

BPTにおいて消去不可傾城として設定した構成とした ので、BPT自体の審き替え処理が防止される。

(図面の簡単な説明)

[図1] 本発明のデータ処理装配の使用概念を説明する 図である。 [図2] 本発明のデータ処理装置のデパイスおよびメデ アの構成を示す図である。

[図3] 本発明のデータ処理装置のメモリ格納データ禍 成を示す図である。

フェースのステータスレジスタのデータ構成を示す図で [図4] 本発明のデータ処理装置にデバイスのメモリイ ンタフェースの詳細構成を示す図である。 【図5】本発明のデータ処理装置におけるメモリインタ

[図6] 本発明のデータ処理装置におけるメディアに格

[図7] 本発明のデータ処理装置においてメディアに格 的されるコンテンツに対応して設定されるセキュリティ 的されるデータの詳細構成を示す図である。

【図8】本発明のデータ処理装置におけるデータ略号化 ヘッグの構成を説明する図である。 の2つの態様を説明する図である。

【図9】 本発明のデータ処理装置におけるリポケーショ ソリストの構成を示す図である。

**パーミッション・テーブル (BPT) について説明する** [図10] 本発明のデータ処理装置におけるブロック

【図12】本発明のデータ処理装置におけるメディア2 【図11】本発明のデータ処理装置におけるメディア1 製造時のBPT格納処理フローを示す図である。 製造時のBPT格柄処理プローを示す図である。

**パトミッション・テープル(BPT)の具体例について** [図13] 本発明のデータ処理装置におけるプロック・ 説明する図である。

[図14] 本発明のデータ処理装置における改竄チェッ [図15] 本発明のデータ処理装置における改竄チェッ 7 値生成処理構成について説明する図である。

[図16] 本発明のデータ処理装置におけるデバイス起 り値検証処理フローについて説明する図である。 り時フローを示す図である。 [図17] 本発明のデータ処理装置におけるファイル割 [図18] 本発明のデータ処理装配におけるメディア1 り当てテーブルの構成例について説明する図である。 8粒時フロー (その1)を示す図である。 [図19] 本発明のデータ処理装置におけるメディア1 【図20】本発明のデータ処理装置におけるメディア2 忍職時フロー(その2)を示す図である。 路職時フロー(その1)を示す図である。 [図21] 本発明のデータ処理装置におけるメディア2 [図22] 本発明のデータ処理装置においてデバイス 忍職時フロー(その2)を示す図である。

メディア何において実行される相互移胚処理シーケンス

[図25] 本発明のデータ処理装置におけるファイルの [図23] 本発明のデータ処理装置における相互認証・ [図24] 本発明のデータ処理装置における相互認能 塑共有処理フロー (その1)を示す図である。 塾共有処理フロー (その2)を示す図である。

[図26] 本発明のデータ処理装置におけるファイルの 筑み出し処理フローを示す図である。 告き込み処理フローを示す図である。

[図27] 本発明のデータ処理装配におけるメモリに格 [図28] 本発明のデータ処理技匠におけるメモリに格 的されたデータの暗号化処理蝦様として適用可能なトリ 的されたデータの暗号化処理態様を説明する図である。 プルDESを説明する図である。

【図31】本発明のデータ処理技匠におけるセクタ対応 コンテンツキー他の鍵の暗号化処理例を説明する図であ [図30] 本発明のデータ処理装置におけるメモリに格 [図32] 本発明のデータ処理協配におけるセクタ対応 【図29】本発明のデータ処理装置におけるメモリに格 **財されたデータの暗号化処理態様を説明する図である。** 的されたデータの時号化処理館様を説明する図である。 改成チェック値の格納処理煽様を説明する図である。

【図33】本発明のデータ処理装配におけるセクタ対応 コンテンツキー他の数の復母処理例を説明する図であ

【図34】本発明のデータ処理装配におけるセクタ対応 コンテンツキー色の製のデバイス・メディア回における 処理例を説明する図である。

【図36】本発明のデータ処理装置におけるファイルの 【図35】本発明のデータ処理装配におけるファイルの [図37] 本発明のデータ処理装配におけるコンテンツ 復号競み出し処理フロー (その1)を示す図である。 復母読み出し処理フロー(その2)を示す図である。 キー他の彼号処理フローを示す図である。

[図38] 本発明のデータ処理装置におけるコンテンツ キー他のメディアの保存塾による彼号処理フローを示す 図である。

【図39】本発明のデータ処理装置におけるセクタデー [図40] 本発明のデータ処理装置におけるセクタデー タの復母処理フロー(その1)を示す図である。

[図41] 本発明のデーク処理装置におけるファイルの [図42] 本発明のデータ処理技匠におけるファイルの [図43] 本発明のデータ処理協匠におけるコンテンツ 苗号化魯を込み処理フロー(その2)を示す図である。 商号化智を込み処理フロー(その1)を示す図である。 ケの復号処理フロー (その2)を示す図である。

[図44] 本発明のデータ処理装置におけるコンテンツ F-他の略号化処理フローを示す図である。

Block #1 Permission Flag Number of Blocks Block #n Permission Flag Format Version メモリインタフェース (1/F) 部 BPT ID ICV of BPT 外部メモリ入出カインタフェース 内部メモリ入出カインタフェース [012] コントロールレジスタ ステータスレジスタ 送信パッファメモリ 受信パッファメモリ コマンドレジスタ アドレスレジスタ カウントレジスタ 送受信制御部 コントローラ 送信レジスタ 受信レジスタ 暗号処理部 暗号処理部 BCC回路 内部メモリ メモリ部 メモリ部 包含的 表示证明 入力回覧 チバイス 230 232 302 305 33 234 301 304 308 35 0 3 236 0.7 401 -- 400 001 -- 380 ¥ ~ E 21 ~ 100 01 - 10 キー他のメディアの保存塾による暗号化処理フローを示 (図47) 本発明のデータ処理装置におけるリポケーションリストの更新処理フローを示す図である。 [図45] 本発明のデータ処理装置におけるセクタデー タの暗号化処理フロー(その1)を示す図である。 【図46】本発明のデータ処理装置におけるセクタデー -10 10 4 Pt 25 タの暗号化処理フロー (その2)を示す図である。 [図1] メモリインタフェース (1/F) 部 [図17] デバイスコントローラ Ĭ Adm á ដ システム運営者 メディア1 メモリ部 212 メモリ部 デバイス デバイス メディア コンチンツの存在・ または システム副指令 复金路 湖価部 表示部 入力部 (符号の説明)・ 14.040 . /04 ディンクトリ ŧ į .0/ .101. 102 300 0.3 200 2 1 0

201 202 204 207

203

202

磁算度を設 B AをAシン 148 148 '164 報い子人 傷引しいチャ 207 Z2Z 母鼠降 16.64.C 164 [23] teiJ naitacoveR 「でく下くに、「やぐ~ Z31 偽い子へ 信不寿 ملائت بالحد (用の)替じ手入 のでなら 一下)時じ手入 「用 # 1/1 (13×1 203 #4Y SOS 母母海 212 300 经制度 ・ロイベロストシィテ 102 2000 LLZ S04

Y2UB\Y05

WE CE

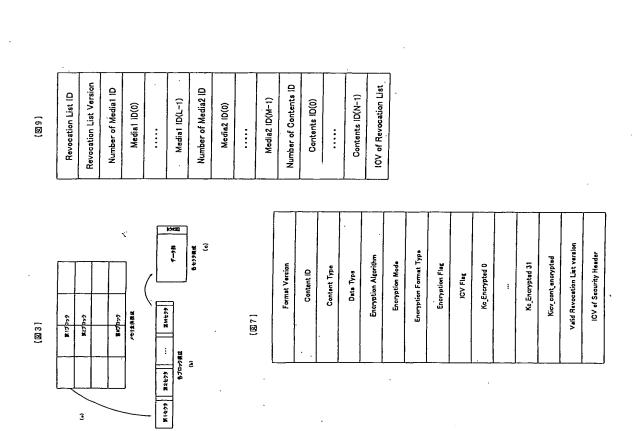
WP [1.8] O\I

RE VIE CIE

(84)

325

324



308

705

353

経回つつヨ

LZE

350

Kdieć Kicv sh. IVsh. MKshe, Vefe Venth. MKsov hy Verse, 1,1Vrt. V kerse, spt. IVso MKsov pst. IVsov spt. IVso

格リチャ

格野政長別

いチャイクやいる是

、TGB くだっかれい もなり 新聞雑器

英是信制物

ATAOR

ATAGW

アドレスレジスタ

**き**たでしはくアロ

そんじしんそーテス

(ATAO)

(PHTD)

#Y

(32)

(P) (B) Contant Content 3 (図 6.) Security Header 3 Content 2 BPCK #2 Security Header 2 Security Header Content 1 Block #3 I finatino D Block #2 Security Header 1 BPCK #1 6K−€3 6K0 2 がd 化動や返費 ででC ST174 ひでで放弃 気まやい たいいが

[EZ 8]

book fi

book fi

book fi

	bbok #1	blook #2	i	block fin-1	block An
eactor Am	Kees of Centers, seeled )	Kancard Content, and Stud 3		Knee jet Carterd, coaffa-13m3)	Knap,ref Centent, technel )
ŧ		1	ï	•	I
sector# 1	Kess, Il Gertert, sep(1)	Rose, 16 Contant, as afare 13.3		Kess, if Cartant, see(in-2)mell )	Kee, If Centent, seutla-13m+13 )
					_

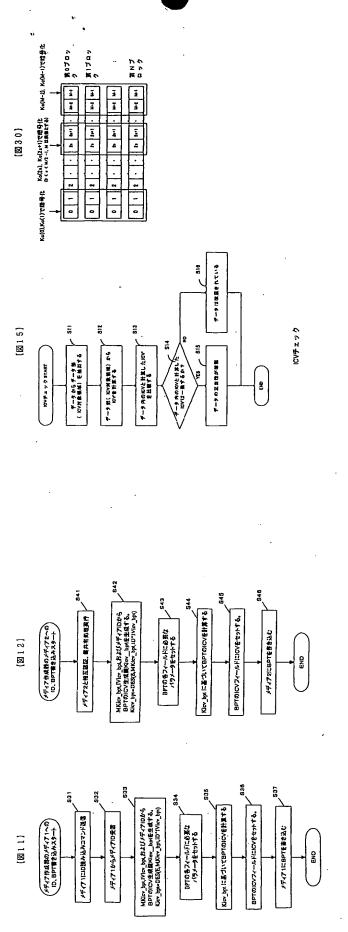
(図13)

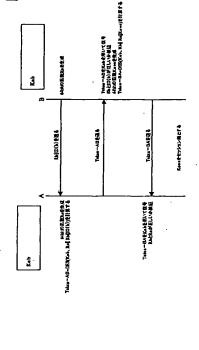
0.消费不可 1.消费利	ンチーマットノージョン	or Fra	7099R	70 p7 1 (Blocket)	プロック2(BheteZ)	70273(Bleedel)	70794(Blocket)	プロック3(Blookes)		7020W(Block/98)	70759(Black#99)	70*2100(B*M100)	ICV of BPT
(e) (g.0 (e) (g.r T98	Oal	1=0	100	1	0	1	-	-	;	-	1	1	0x1234
				<b>†</b>	1	1	-	<b>†</b>		1	1	1	
•			4417047	ファイル相が当てキーブル	i i	707941	707341	プログラム2		7-51	1	1	
				(190ctor) (Bloctor)	70-92(Block#1)	70723(Blocket)	JOSSA (Nincipal)	70773(Block#3)		712-9796(Blocke96)	JD-2599 (Block#99)	7027100(810036100)	•

(38)

(31)

(88)





(822)

(図14)

ICVMRF-9 ICV

ISO/ISC 9798-2. 对称程度号技術を用いた相互認証および競技者方式

コンナンツチェックは: ICV

וכא' =וכא?

・体性的性質和效理(8)(小・単位)

107年度、食品方法

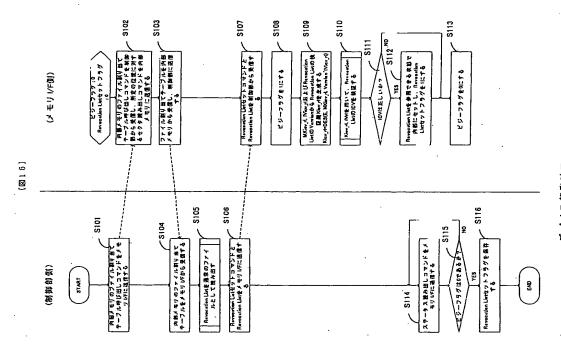
iCVRIER DES

**E** 

(33)

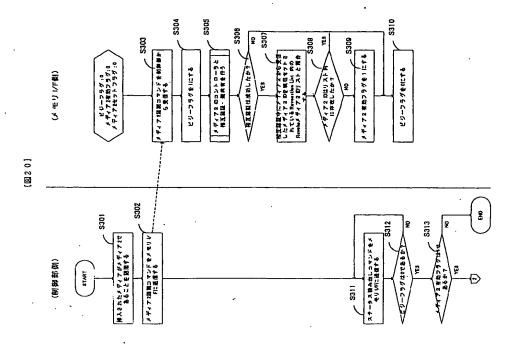
(42)

メディア 1 認識時フロー



デパイス起動時フロー





(メモリ //F側)

(監督等急)

[612]

S223

ファイル部リ当でテーブルモメ ディア1から受信し、例如節に送 信する

S224

S227

S228

BPTセットコマンドとBPTをメモリ VFIに出席する

S225

BPTを選集のファイルとして 競を出す

メディアコ のファイル割り 当て・一フ ルモメモリ いたから 更属する

BPTセントコマンドトBPTを司召集 から収録する

ピジーフラグをルにする

\$231

CVILE L UB 7

Kiov, bot, Montを用いて、BPTのIOVを独在する

\$232

OPFを参加できる状態で内別に セットし、メディア」セットフラ グを1にする

ピジーフラグを012する

, S236

メディアーセットワラグを保存する

Š

S235

- 13 7 HOT & 6 #

メディア1 認齳時フロー ( cont. )

(43)

<del>(4</del>

[图23]

(46)

2

S333

ビジーンラグをのこする

S338

メディア2 セットフラグを係存する

( <u>a</u>

ステータス数を出しコマンドキメモリ びに恐怖する

相互認証・盤共有フロー

. \$323

ファイル部リ当でテーブルキメディアとから映画し、 気容器に改善する

メディア2 のファイル取り 当て テーフルをメモリ VFから 受信する

DPTを現在のファイルとして 報か出す S327

BPTセットコマンドとBPTを制設的 から美価する

\$325

BP1セットコマンドとBP1モノモリ VFに送信する S328

ピジーフラグをにてる

8338

MKJev, Det. Mav, bat B 上 U 乡 千 7 丁 2 のむから BPTの 株 延 MKIvo, bat を 生 成 寸 も Kiov, bat DES(E, MKivo, bat, BX)

Kiev, bet, Mace, All. C., 8910.

ICV社正しいか?

S322

(メモリ/F倒)・

(室智哲堂)

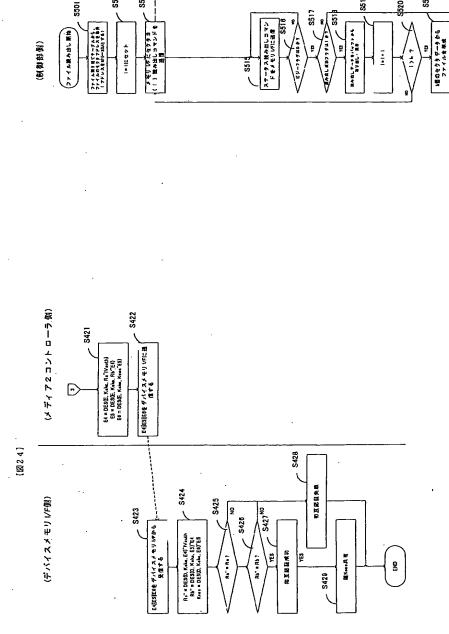
[図21]

メディア2 認慎時フロー ( oont. )

(46)

(メモリ (/F側)

(図25)



**S**506

ピターフラグもこにセット

セクタの(一) 数み出しコマンドを実施

√ S503

, S502

1-16427

S20

**登録と担いませて イル** 

(重智哲學)

フロー 1-4:相互認証・鍵共有フロー (oont.)

ファイ ルの読み出し 処理

味みかし メネフラグそりになかり

まんむし ほぞうし かれこにセット 関チ近し 最近の (シッピにカット

:

ピジーフラグをのにセット

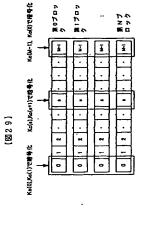
\$521

\ \ \ \ \

工工各位五批 计图像转形工

(48)

(図27)



(99)

DBS 再号化

S613

ピジーフラグをのにセット

2882

7 S621

ファイルボンガハヤーブルに参き込み位権を反驳

S620

5810

#1702 至のプロック Ko(a)で数年に Ko(M-1)で番号化 DES FFFF [828] ■ 以外の子ータ Kc(0) Kd(1) .. Ka(0)で配事化 3

セクタ8(!) 事を込みコ マンド 未受信

\$604

セクタリ(1) 春を込みコーマンドとゲータロ(1) を 送用

S618

\$600

(一) を着き込むゼクタ S(1) を決定

**S802** 

1-11:42 F

ピジーフラグを1にセット

ファイルの書き込み処理

(49)

特朗2002-132583

(メモンI/F側)

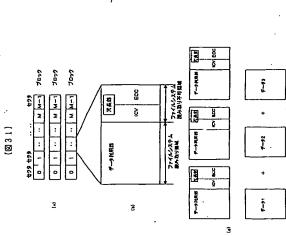
S801

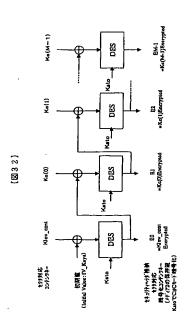
77411 BE WAR

(制度物金)

ファイルをセクタに分割し データをO(!)~D Nと t)

(**Ø**26)





(834)

(29)

(図36)

. 3722

5723

見み出し よかつりがそのにセット

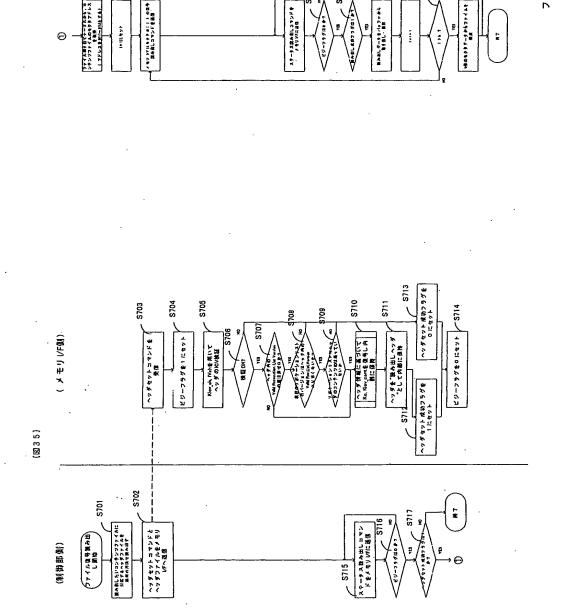
取りおし 成ねつ リグラッドセット おおさんな データ ボラ・シッド カット

S748

ファイルの復号読み出し処理

8734

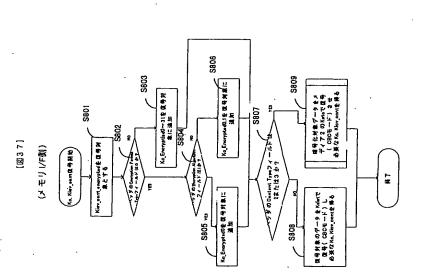
S743 S744



S730 S731

ファイルの復号読み出し処理

[图38]



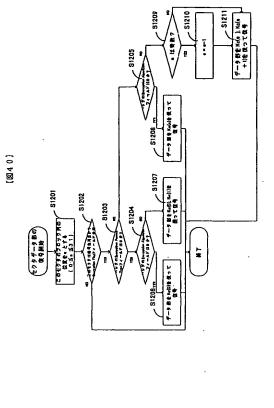
(メディア2 ロントローリ色) メモリ UFÞ5 ゲータ KDE 東住 レジスタに砂湖路Niewを セット Kataに関ム的の出しド による契号 保与された親子―9 取得 1925 2977 10-Xが元10年 N Laye 最初 報とし Kee・を使って OBCモードで戦争 \_ S1003 S1004 11018 J S1013 \_ S1012 . \$1010 CBC関号初期化コマンド設備 色の オントコート 数数 (メモリ/F側) 展テータの復母 KON 斑点 このを発信 :

復号対象データをメディア2 のKstoで復号

(29)

フロー 4-3:Ka, Kiov\_contの復号

[833]



セクタデータ 即の復号(その1)

セクタデータ節の復号(その2)

(メモリ VF側)

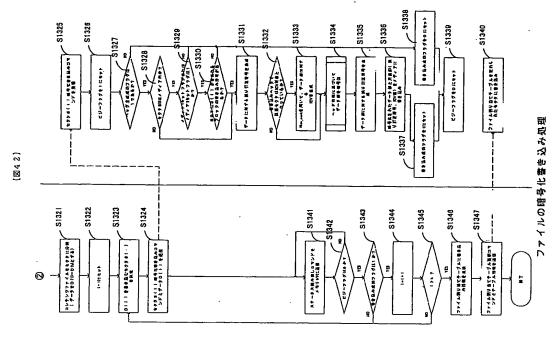
27.4.比較年化等者 込み開始

(多数年度)

(図41)

しょ が形成り トンド も来信

ピジーフラグモリにセット



S1306

ヘッタ供職に基づいて Ko. Kov\_contを生成・歴 毎化 \$1307

. \$1311

S1314

ヘッダ 生成成功フラグを1 にセット 生成されたヘッダをパッ ファにセット

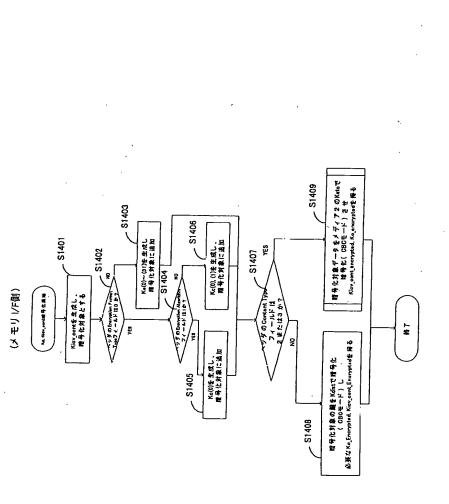
S1309 |

ピジーフラグをロにセット

ファイルの暗号化書き込み処理

[图44]

(🖾 43)



Ke, Kiev\_contの暗号化

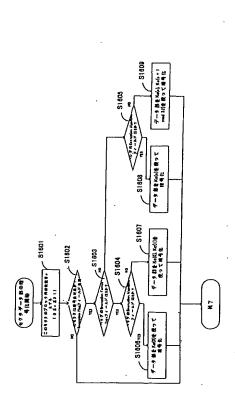
J S1510 J S1515 (ダ ディア2コントローリ室) 女キナーケッド こうたののこう カード かばるもだし トス・ハーン かがあった アン・ス・ハーン でがあった かん 1197745 F-51 (11 488 KOE Kusto Bot -- Fr R4 レジスタモクリア BARN Sert √ S1505 J S1512 S1504 . \$1501 \$1511 \_ S1502 . \$1503 J S1514 S1513 森中で対象の銀ケーケル X(0)-X(n-1)とする CRC単元で記載のマンド組織 CBC年7コマンド 祝母 田子―今の昭春化 (メモリルF側) 元()を出席 大・0代 東部 : -

暗号化対象データをメディア2のKstoで暗号化

(62)

[🖾46]

[🖾 4 5]



セクタ データ 部の暗号化(その1)

セクタデータ郜の暗号化(その2)



[847]

(12)発明者 秋下 松 東京都品川区北品川6丁目7番35号 ソニ 一株式会社内 (72)発明者 白井 太三 中株式会社内 (72)発明者 は 茂和 東京都品川区北品川6丁目7番35号 ソニ 一株式会社内 上株式会社内 上株式会社内 アクーム(参考) 55017 AMOI RNOI RCO4 Fクーム(参考) 55017 AMOI RNOI RCO4 RCO8 CCO4 CCO8 DE17 DE50 FG18 CX11 III113 III115 JJD3

> , S1803 \$1805 \$1806 \$1804 \$1807 S1809 RE to > 2 tttl S Resention ListO Version ( LT 6 ) 2 EM R Remodiful ListO Version ( LT 6 ) TES TRANSPORTED TES ILLE A MILLON TES ILLE TES MKbryt Ward およけぎ町用 Revealor Let Ø Verbath ら mouton Let Ø 教廷 最Kbryt を生成 する 医療器 Revocation Listチェックロマンドと 医軟用 Revocation Listや自然 響から 製造する Kev-Livie 用いて、更新用 Reveable ListのICVを依旧する ピジーフラグをにする ビジーフラグをのにする (メモリ //F側) いるいつ場んでは CV(本正しいか? ANDESSE MIKE Revocation Listの更新 J S1814 . S1815<sup>NO</sup> \$1813 TES SION TES SION DIE AND DI 東新用のRevestion Lette 過程制か 与安陽する 逆節器Reveation Listチェックコマンドと更更無Reveation Listをよるリンドと更更無Beveation Listをよるリンドに処国する ステータス 彼み出しコマンドセメモリ レドに送信する E#用Reventan Lath 数子 - 23 7 Have 16 6 8 (知知部息) 37.ART 8 S1812

(99)

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

FADED TEXT OR DRAWING

BLURRED OR ILLEGIBLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

## IMAGES ARE BEST AVAILABLE COPY.

☐ OTHER:

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.